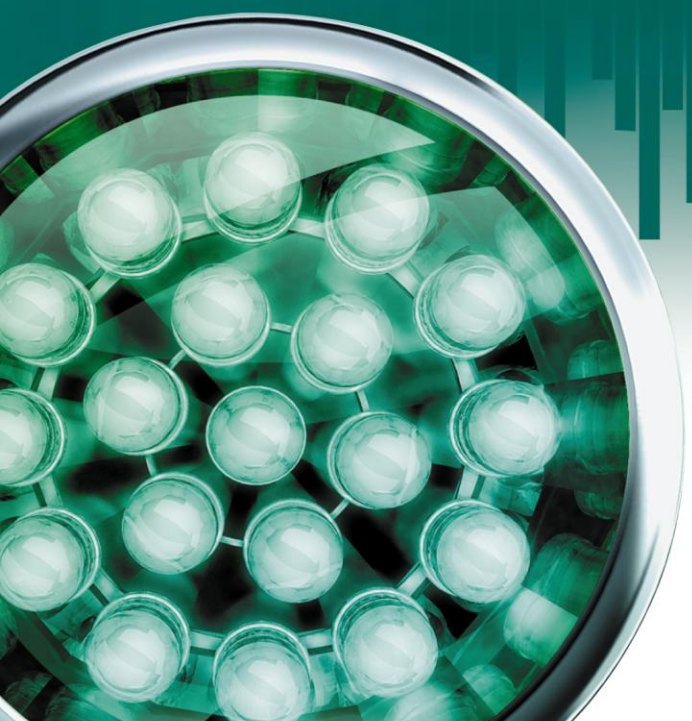
Kaspersky PURE

BENUTZERHANDBUCH

PROGRAMMVERSION: 9.1



KASPERSKY lab

Sehr geehrter Benutzer!

Vielen Dank, dass Sie unser Produkt ausgewählt haben. Wir hoffen, dass diese Dokumentation Ihnen hilft und die meisten Fragen damit beantwortet werden können.

Wichtiger Hinweis: Die Rechte an diesem Dokument liegen bei Kaspersky Lab und sind durch die Urhebergesetze der Russischen Föderation und durch internationale Abkommen geschützt.

Bei illegalem Vervielfältigen und Weiterverbreiten des Dokuments oder einzelner Teile daraus kann der Beschuldigte nach geltendem Recht zivilrechtlich, verwaltungsrechtlich und strafrechtlich zur Verantwortung gezogen werden.

Das Dokument und dazu gehörenden Grafiken dürfen nur zu informativen, nicht gewerblichen oder persönlichen Zwecken gebraucht werden.

Das Dokument darf ohne vorherige Benachrichtigung geändert werden. Die neueste Version finden Sie auf der Seite von Kaspersky Lab unter der Adresse http://www.kaspersky.com/de/docs.

Für den Inhalt, die Güte, Aktualität und Richtigkeit der im Dokument verwendeten Unterlagen, deren Rechte anderen Rechteinhabern gehören, sowie für den möglichen Schaden durch die Nutzung dieser Unterlagen, lehnt Kaspersky Lab die Haftung ab.

In diesem Dokument werden eingetragene Markenzeichen und Handelsmarken verwendet, die das Eigentum der jeweiligen Rechtsinhaber sind.

Redaktionsdatum: 14.09.2010

© 1997-2010 Kaspersky Lab ZAO. Alle Rechte vorbehalten.

http://www.kaspersky.de
http://support.kaspersky.com/de/

INHALT

ENDNUTZER-LIZENZVERTRAG FÜR KASPERSKY LAB SOFTWARE 12

ÜBER DIESES HANDBUCH 19

In diesem Dokument 19

Formatierung mit besonderer Bedeutung 20

ZUSÄTZLICHE INFORMATIONSQUELLEN 22

Informationsquellen zur selbständigen Recherche 22

Diskussion über die Programme von Kaspersky Lab im Webforum 23

Kontaktaufnahme mit der Vertriebsabteilung 23

Kontakt zur Abteilung für Handbücher und Hilfesysteme 23

KASPERSKY PURE 24

Lieferumfang 24

Organisation des Schutzes für ein Heimnetzwerk 25

Service für registrierte Benutzer 27

Hard- und Softwarevoraussetzungen 28

PROGRAMM INSTALLIEREN UND DEINSTALLIEREN 29

Installation des Programms auf einem Computer 30

Schritt 1. Nach neuer Programmversion suchen 31

Schritt 2. Systemkompatibilität für Installation prüfen 32

Schritt 3. Installationstyp auswählen 32

Schritt 4. Lizenzvereinbarung anzeigen 32

Schritt 5. Erklärung zur Verwendung von Kaspersky Security Network 32

Schritt 6. Zielordner auswählen 33

Schritt 7. Programmkomponenten für Installation auswählen 33

Schritt 8. Nach anderen Antiviren-Anwendungen suchen 34

Schritt 9. Firewall von Microsoft Windows deaktivieren 34

Schritt 10. Installation vorbereiten 34

Schritt 11. Installation 35

Schritt 12. Programm aktivieren 35

Schritt 13. Daten überprüfen 35

Schritt 14. Anmeldung des Benutzers 35

Schritt 15. Aktivierung abschließen 36

Schritt 16. Kontrolle des Zugriffs auf das Programm 36

Schritt 17. Schutzmodus auswählen 36

Schritt 18. Programm-Update anpassen 37

Schritt 19. Erkennbare Bedrohungen auswählen 37

Schritt 20. Systemanalyse 38

Schritt 21. Assistent abschließen 38

Erste Schritte 39

Programm mit Hilfe des Installationsassistenten ändern, reparieren oder löschen 40

Schritt 1. Startfenster des Installationsprogramms 40

Schritt 2. Operation wählen 40

Schritt 3. Operation zum Reparieren, Ändern oder Löschen des Programms abschließen 41

LIZENZVERWALTUNG 42

Über den Lizenzvertrag 42

Über die Lizenz....42
Über den Aktivierungscode....43
Lizenz-Info anzeigen....43
PROGRAMMOBERFLÄCHE....45
Symbol im Infobereich der Taskleiste....45
Kontextmenü....46
Hauptfenster von Kaspersky PURE....47
Computersicherheit....49
Backup....50
Kindersicherung....51
Fenster von Password Manager....52
Symbol im Infobereich der Taskleiste....52
Kontextmenü von Password Manager....53
Fenster der Kennwort-Datenbank....53
Konfigurationsfenster....54
Titelleisten-Schaltfläche....55
Erweiterungen und Plug-ins....55
Zeiger....55
Programmkonfigurationsfenster....55
Meldungsfenster und Popupmeldungen....56
PROGRAMM STARTEN UND BEENDEN....58
Automatischen Start aktivieren und deaktivieren....58
Programm manuell starten und beenden....58
STATUS DES SCHUTZES FÜR EIN HEIMNETZWERK....59
Probleme im Schutz diagnostizieren und beheben....59
Computerschutz aktivieren/deaktivieren....60
Schutz anhalten....61
Interaktiven Schutzmodus verwenden....61
LÖSUNGEN FÜR TYPISCHE AUFGABEN....63
Wie das Programm aktiviert wird.....63
Lizenzerwerb oder -verlängerung....64
Was tun, wenn das Programm Meldungen anzeigt?....65
Aktualisierung von Programmdatenbanken und -modulen....65
Wie wichtige Computerbereiche auf Viren untersucht werden.....65
Untersuchung von Dateien, Ordnern, Laufwerken und anderen Objekten auf Viren....66
Wie eine vollständige Virenuntersuchung des Computers ausgeführt wird.....68
Wie der Computer auf Schwachstellen untersucht wird.....68
Wie der Schutzstatus für ein Heimnetzwerk ferngesteuert geprüft wird....69
Wie Ihre persönlichen Daten vor Diebstahl geschützt werden....70
Schutz vor Phishing....70
Virtuelle Tastatur....71
Password Manager....71
Datenverschlüsselung....72
Was tun, wenn Sie vermuten, dass ein Objekt von einem Virus infiziert ist?....73
Wie ein Objekt wiederhergestellt wird, das vom Programm gelöscht oder desinfiziert wurde.....74
Was tun, wenn Sie vermuten, dass Ihr Computer infiziert ist?....74
Wie Sicherungskopien Ihrer Daten angelegt werden....76

Wie der Zugriff auf die Einstellungen von Kaspersky PURE eingeschränkt wird 77
Wie die Verwendung des Computers und Internets für verschiedene Benutzer eingeschränkt wird 78
Wie eine Notfall-CD erstellt und verwendet wird 78
Notfall-CD erstellen 79
Hochfahren eines Computers mit Hilfe der Notfall-CD 80
Wie mit einer großen Anzahl von Spam-Mails verfahren wird? 80
Wie ein Bericht über den Computerschutz geöffnet wird 82
Wie die Standardeinstellungen des Programms wiederhergestellt werden 82
Wie die Programmeinstellungen auf einen anderen Computer übertragen werden 83

ERWEITERTE PROGRAMMEINSTELLUNGEN 84
Computersicherheit 85
Untersuchung des Computers 85
Virensuche 86
Suche nach Schwachstellen 93
Update 93
Updatequelle auswählen 95
Zeitplan für Updatestart erstellen 97
Rollback zum vorherigen Update 98
Untersuchung der Quarantäne nach dem Update 98
Proxyserver verwenden 98
Updatestart mit den Rechten eines anderen Benutzers 99
Datei-Anti-Virus 99
Datei-Anti-Virus aktivieren und deaktivieren 100
Datei-Anti-Virus automatisch anhalten 100
Schutzbereich festlegen 101
Sicherheitsstufe ändern und wiederherstellen 102
Untersuchungsmodus ändern 103
Heuristische Analyse verwenden 103
Untersuchungstechnologie 104
Aktion für gefundene Objekte ändern 104
Untersuchung von zusammengesetzten Dateien 104
Untersuchung optimieren 105
Mail-Anti-Virus 106
Mail-Anti-Virus aktivieren und deaktivieren 107
Schutzbereich festlegen 107
Sicherheitsstufe ändern und wiederherstellen 108
Heuristische Analyse verwenden 109
Aktion für gefundene Objekte ändern 109
Anlagenfilterung 109
Untersuchung von zusammengesetzten Dateien 110
E-Mail-Untersuchung in Microsoft Office Outlook 110
E-Mail-Untersuchung in The Bat! 110
Web-Anti-Virus 111
Web-Anti-Virus aktivieren und deaktivieren 113
Sicherheitsstufe ändern und wiederherstellen 113
Aktion für gefundene Objekte ändern 114
Gefährliche Skripts blockieren 114
Link-Untersuchung mit den Datenbanken für verdächtige und Phishing-Adressen 114

Heuristische Analyse verwenden 115
Untersuchung optimieren 115
Modul zur Link-Untersuchung 116
Liste mit vertrauenswürdigen Adressen erstellen 117
IM-Anti-Virus 117
IM-Anti-Virus aktivieren und deaktivieren 118
Schutzbereich festlegen 118
Untersuchungsmethode auswählen 118
Anti-Spam 119
Anti-Spam aktivieren und deaktivieren 121
Sicherheitsstufe ändern und wiederherstellen 121
Anti-Spam-Training 122
Links in Nachrichten untersuchen 125
Spam nach Phrasen und Adressen ermitteln. Listen erstellen 125
Grenzwerte für den Spam-Faktor regulieren 130
Zusätzliche Merkmale für die Spam-Filterung verwenden 131
Algorithmus zur Spam-Erkennung auswählen 131
Markierung zum Betreff einer Nachricht hinzufügen 132
Filterung von E-Mails auf dem Server. Mail-Manager 132
Nachrichten für Microsoft Exchange Server von der Untersuchung ausschließen 133
Spam-Verarbeitung in Mailprogrammen anpassen 133
Anti-Banner 136
Anti-Banner aktivieren und deaktivieren 136
Untersuchungsmethoden wählen 137
Listen für verbotene und erlaubte Banneradressen erstellen 137
Adressenlisten exportieren / importieren 137
Programmkontrolle 138
Programmkontrolle aktivieren und deaktivieren 139
Programme zu Gruppen zuordnen 140
Aktivität von Programmen anzeigen 141
Sicherheitsgruppe ändern 141
Regeln für die Programmkontrolle 142
Schutz für Betriebssystemressourcen und persönliche Daten 146
Proaktiver Schutz 147
Proaktiven Schutz aktivieren und deaktivieren 147
Gruppe mit vertrauenswürdigen Programmen erstellen 148
Liste der gefährlichen Aktivität verwenden 148
Kontrollregel für gefährliche Aktivität ändern 148
Rollback von Aktionen eines schädlichen Programms 149
Netzwerkschutz 149
Firewall 151
Schutz vor Netzwerkangriffen 154
Untersuchung geschützter Verbindungen 157
Netzwerkmonitor 159
Proxyserver-Einstellungen 159
Liste der zu kontrollierenden Ports erstellen 160
Vertrauenswürdige Zone 161
Liste mit vertrauenswürdigen Programmen erstellen 162
Ausnahmeregeln erstellen 162

Sichere Umgebung für die Ausführung von Programmen....164
Start eines Programms in der Sicheren Umgebung....164
Liste der Programme erstellen, die in der Sicheren Umgebung gestartet werden sollen....165
Verknüpfung für den Start von Programmen erstellen....166
Daten der Sicheren Umgebung bereinigen....166
Gemeinsamen Ordner verwenden....167
Quarantäne und Backup....168
Quarantäne- und Backup-Objekte speichern....168
Arbeit mit Objekten in der Quarantäne....169
Backup....171
Speicher anlegen....171
Bereits vorhandenen Speicher verbinden....172
Speicher leeren....172
Speicher löschen....173
Backup-Aufgabe erstellen....173
Backup starten....174
Daten wiederherstellen....174
Sicherungskopien suchen....175
Daten einer Sicherungskopie anzeigen....176
Ereignisbericht anzeigen....177
Kindersicherung....178
Kindersicherung für einen Benutzer anpassen....179
Kontrolle aktivieren und deaktivieren....179
Einstellungen der Kindersicherung speichern und laden....179
Darstellung eines Benutzerkontos in Kaspersky PURE....180
Arbeitszeit auf dem Computer....181
Start von Programmen....181
Arbeitszeit im Internet....181
Besuch von Webseiten....182
Download von Dateien aus dem Internet....182
Modus für sichere Suche....182
Korrespondenz über Instant Messenger....183
Korrespondenz in sozialen Netzwerken....184
Senden vertraulicher Informationen....185
Schlüsselwörter suchen....186
Berichte über die Aktionen eines Benutzers anzeigen....186
Datenverschlüsselung....187
Bereits vorhandenen Speicher erstellen und verbinden....187
Zugriff auf Daten in einem Container blockieren und freigeben....188
Dateien zu einem Container hinzufügen....189
Einstellungen eines Containers anpassen....189
Verknüpfung für den schnellen Zugriff auf einen Container erstellen....190
Verwaltung....191
Fernverwaltung anpassen....191
Untersuchung eines Heimnetzwerks auf Viren und Schwachstellen....192
Remote-Update der Datenbanken auf Netzwerkcomputern....192
Schutzkomponenten auf Netzwerkcomputern aktivieren / deaktivieren....193
Kindersicherung fernverwalten....193
Backup auf Netzwerkcomputern starten....194

Remote-Verwaltung von Lizenzen auf Netzwerkcomputern 194
Password Manager 195
Kennwort-Datenbank verwalten 196
Zugriff auf die Kennwort-Datenbank 196
Persönliche Daten hinzufügen 197
Persönliche Daten verwenden 205
Kennwörter suchen 205
Persönliche Daten löschen 206
Daten importieren/exportieren 206
Backup / Wiederherstellung der Kennwort-Datenbank 208
Programmparameter anpassen 210
Konfigurationsassistent 211
Standardmäßigen Benutzernamen verwenden 211
Häufig verwendete Benutzerkonten 212
Ignorierte Webadressen 213
Vertrauenswürdige Webadressen 213
Tastenkombination 214
Ort der Kennwort-Datenbank 214
Neue Kennwort-Datenbank anlegen 215
Speicherort für eine Sicherungskopie 216
Verschlüsselungsmethode auswählen 217
Kennwort-Datenbank automatisch blockieren 218
Authentifizierungsmethode für Password Manager ändern 218
USB- oder Bluetooth-Geräte zur Authentifizierung verwenden 219
Master-Kennwort ändern 219
Unterstützte Webbrowser 220
Vorlagen für persönliche Notizen verwalten 220
Titelleisten-Schaltfläche anzeigen 221
Speicherdauer des Kennworts in der Zwischenablage 222
Meldungen 222
Aktion bei Doppelklick 223
Erstellen von sicheren Kennwörtern 223
Verwendung einer portablen Version des Password Managers 224
Portable Version erstellen und verbinden 224
Synchronisierung der Kennwort-Datenbank 225
Leistung und Kompatibilität mit anderen Programmen 226
Kategorien der erkennbaren Bedrohungen auswählen 227
Technologie zur Desinfektion einer aktiven Infektion 227
Verteilung der Computerressourcen bei der Virensuche 228
Programmparameter bei der Arbeit im Vollbildmodus. Profil für Spiele 228
Energiesparen im Akkubetrieb 229
Selbstschutz für Kaspersky PURE 229
Selbstschutz aktivieren und deaktivieren 230
Schutz vor externer Steuerung 230
Aussehen des Programms 230
Aktive Elemente der Benutzeroberfläche 231
Grafische Oberfläche von Kaspersky PURE 231
News Agent 231
Zusätzliche Funktionen 233

Unwiderrufliches Löschen von Daten ... 234
Aktivitätsspuren löschen ... 235
Nicht verwendete Informationen löschen ... 236
Browser-Konfiguration ... 238
Berichte ... 239
Bericht für eine bestimmte Komponente erstellen ... 240
Datenfilterung ... 240
Suche nach Ereignissen ... 241
Bericht in Datei speichern ... 242
Berichte speichern ... 242
Berichte leeren ... 243
Nicht kritische Ereignisse protokollieren ... 243
Erinnerung an die Bereitschaft eines Berichts anpassen ... 243
Meldungen ... 244
Benachrichtigungen aktivieren und deaktivieren ... 244
Benachrichtigungsmethode anpassen ... 244
Teilnahme an Kaspersky Security Network ... 245
EINSTELLUNGEN VON KASPERSKY PURE AUF KORREKTHEIT PRÜFEN ... 247
EICAR-"Testvirus" und seine Modifikationen ... 247
Testen des Schutzes für HTTP-Datenverkehr ... 249
Schutz für den SMTP-Datenverkehr testen ... 249
Überprüfung der Einstellungen von Datei-Anti-Virus ... 249
Überprüfung der Einstellungen für eine Aufgabe zur Virensuche ... 250
Überprüfung der Einstellungen für den Schutz vor unerwünschten E-Mails ... 250
KONTAKTAUFNAHME MIT DEM TECHNISCHEN SUPPORT ... 251
Mein Kaspersky Account ... 251
Technischer Support am Telefon ... 252
Bericht über den Systemstatus erstellen ... 252
Protokolldatei erstellen ... 253
Dateien mit Daten senden ... 253
AVZ-Skript ausführen ... 254
ANHÄNGE ... 256
Varianten für den Abo-Status ... 256
Bedienung des Programms über die Befehlszeile ... 257
Programm aktivieren ... 258
Programm starten ... 259
Programm beenden ... 259
Steuerung von Komponenten und Aufgaben des Programms ... 259
Virensuche ... 261
Programm-Update ... 263
Rollback zum vorherigen Update ... 264
Schutzparameter exportieren ... 264
Schutzparameter importieren ... 265
Protokolldatei anlegen ... 265
Hilfe anzeigen ... 266
Rückgabecodes der Befehlszeile ... 266
Liste der Benachrichtigungen von Kaspersky PURE ... 267
Desinfektion des Objekts ist nicht möglich ... 267

Nicht verfügbarer Updateserver 268
Verdächtiges Objekt wurde gefunden 268
Gefährliches Objekt wurde im Datenstrom gefunden 269
Verdächtiges Objekt wurde gefunden 269
Gefährliche Aktivität im System wurde erkannt 270
Versteckter Prozess wurde gefunden 271
Versuch zum Zugriff auf die Systemregistrierung wurde erkannt 271
Netzwerkaktivität eines Programms wurde erkannt 272
Neues Netzwerk wurde gefunden 273
Phishing-Angriff wurde erkannt 273
Verdächtiger Link wurde gefunden 273
Ein inkorrektes Zertifikat wurde gefunden 274
Zeitbeschränkung für die Verwendung eines Programms 274
Spezielle Desinfektionsprozedur ist erforderlich 274
Die Datei ist bereits vorhanden 274

GLOSSAR 276

KASPERSKY LAB 286

INFORMATIONEN ZUM CODE VON DRITTHERSTELLERN 287
Programmcode 287
AGG (ANTI-GRAIN GEOMETRY) 2.4 288
BISON PARSER SKELETON 2.3 289
BOOST 1.30.0, 1.39.0, 1.43.0 289
BZIP2/LIBBZIP2 1.0.5 290
EXPAT 1.2, 2.0.1 290
FASTSCRIPT 1.9 290
GECKO SDK 1.8 290
INFO-ZIP 5.51 290
LIBJPEG 6B 291
LIBNKFM 2.0.5 292
LIBPNG 1.2.8, 1.2.29 292
LIBSPF2 1.2.9 292
LIBUNGIF 3.0 293
LIBXDR 293
NDIS INTERMEDIATE MINIPORTDRIVER SAMPLE 293
NDIS SAMPLE NDIS LIGHTWEIGHT FILTER DRIVER 294
NETWORK CONFIGURATION SAMPLE 294
OPENSSL 0.9.8D 294
PCRE 3.0, 7.4, 7.7 295
PROTOCOL BUFFER 296
QT 4.6.1 296
RFC1321-BASED (RSA-FREE) MD5 LIBRARY 302
TINICONV 1.0.0 302
WINDOWS TEMPLATE LIBRARY 7.5 307
WINDOWS TEMPLATE LIBRARY 8.0 310
ZLIB 1.2, 1.2.2 310
Sonstige Informationen 310

SACHREGISTER.....311

ENDNUTZER-LIZENZVERTRAG FÜR KASPERSKY LAB SOFTWARE

WICHTIGER RECHTLICHER HINWEIS AN ALLE NUTZER: LESEN SIE FOLGENDE RECHTLICHE VEREINBARUNG SORGFÄLTIG DURCH, BEVOR SIE DIE SOFTWARE NUTZEN.

INDEM SIE IM LIZENZVERTRAG-FENSTER AUF DIE SCHALTFLÄCHE AKZEPTIEREN KLICKEN ODER EIN ENTSPRECHENDES ZEICHEN BZW. ENTSPRECHENDE ZEICHEN EINGEBEN, ERKLÄREN SIE SICH MIT DER EINHALTUNG DER GESCHÄFTSBEDINGUNGEN DIESES VERTRAGS EINVERSTANDEN. **DIESE AKTION KONSTITUIERT EIN BEKENNTNIS IHRER SIGNATUR UND SIE STIMMEN DIESER VEREINBARUNG, UND DASS SIE EINE PARTEI DIESER VEREINBARUNG WERDEN, ZU UND ERKLÄREN SICH WEITERHIN EINVERSTANDEN, DASS DIESE VEREINBARUNG, WIE JEDWEDE ANDERE SCHRIFTLICHE, AUSGEHANDELTE UND DURCH SIE UNTERZEICHNETE VEREINBARUNG AUCH, VOLLSTRECKBAR IST.** SOLLTEN SIE MIT DEN GESCHÄFTSBEDINGUNGEN DIESER VEREINBARUNG NICHT EINVERSTANDEN SEIN, BEENDEN SIE DIE INSTALLATION DER SOFTWARE BZW. INSTALLIEREN SIE SIE NICHT.
NACHDEM SIE IM LIZENZVERTRAG-FENSTER AUF DIE SCHALTFLÄCHE AKZEPTIEREN GEKLICKT ODER EIN ENTSPRECHENDES ZEICHEN BZW. ENTSPRECHENDE ZEICHEN EINGEGEBEN HABEN, SIND SIE BERECHTIGT, DIE SOFTWARE IM EINKLANG MIT DEN GESCHÄFTSBEDINGUNGEN DIESER VEREINBARUNG ZU NUTZEN.

1. **Definitionen**
1.1. **Software** bezeichnet Software einschließlich aller Updates und zugehöriger Materialien.
1.2. **Rechtsinhaber** (Inhaber aller Rechte an der Software, ob exklusiv oder anderweitig) bezeichnet Kaspersky Lab ZAO, ein gemäß den Gesetzen der Russischen Föderation amtlich eingetragenes Unternehmen.
1.3. **Computer** bezeichnet/bezeichnen Hardware, einschließlich von PCs, Laptops, Workstations, PDAs, Smart Phones, tragbaren oder sonstigen elektronischen Geräten, für welche die Software konzipiert war und auf denen die Software installiert und/oder verwendet werden wird.
1.4. **Endnutzer (Sie)** bezeichnet eine bzw. mehrere Personen, die die Software in eigenem Namen installieren oder nutzen, oder die eine Software-Kopie rechtmäßig nutzt/nutzen, oder, falls die Software im Namen einer Organisation heruntergeladen oder installiert wurde, wie etwa einem Arbeitgeber, bezeichnet der Begriff *„Sie“* weiterhin jene Organisation, für die die Software heruntergeladen oder installiert wird, und es wird hiermit erklärt, dass eine solche Organisation die diese Vereinbarung akzeptierende Person autorisiert hat, dies in ihrem Namen zu tun. Im Sinne dieses Lizenzvertrags beinhaltet der Begriff *„Organisation“* ohne Einschränkungen jedwede Partnerschaft, GmbH, Gesellschaft, Vereinigung, Aktiengesellschaft, Treuhandgesellschaft, Gemeinschaftsunternehmen, Arbeitsorganisation, nicht eingetragene Organisation oder staatliche Behörde.
1.5. **Partner** bezeichnet Organisationen oder Personen, die die Software auf Grundlage eines Vertrags und einer mit dem Rechtsinhaber vereinbarten Lizenz vertreiben.
1.6. **Update(s)** bezeichnet/n alle Upgrades, Korrekturen, Patches, Erweiterungen, Reparaturen, Modifikationen, Kopien, Ergänzungen oder Wartungs-Softwarepakete usw.
1.7. **Benutzerhandbuch** bezeichnet die Bedienungsanleitung, die Administrator-Anleitung, ein Nachschlagewerk und ähnliche erläuternde oder sonstige Materialien.

2. Lizenzgewährung
2.1. Der Rechtsinhaber gewährt Ihnen hiermit eine nicht-ausschließliche Lizenz zur Speicherung, zum Laden, zur Installation, Ausführung und Darstellung (zur „Nutzung“) der Software auf einer festgelegten Anzahl von Computern zur Unterstützung des Schutzes Ihres Computers, auf dem die Software installiert ist, vor im Nutzerhandbuch beschriebenen Bedrohungen gemäß den technischen, im Benutzerhandbuch beschriebenen Anforderungen und im Einklang mit den Geschäftsbedingungen dieses Vertrags (die „Lizenz“). Sie erkennen diese Lizenz an.
Testversion. Sollten Sie eine Testversion der Software erhalten, heruntergeladen und/oder installiert haben und sollte Ihnen hiermit eine Evaluierungslizenz für die Software gewährt worden sein, dürfen Sie die Software ab dem Datum der ersten Installation nur zu Evaluierungszwecken verwenden, und zwar

ausschließlich während der einzigen geltenden Evaluierungsperiode, außer wie anderweitig angegeben. Jegliche Nutzung der Software zu anderen Zwecken oder über die geltende Evaluierungsperiode hinaus ist strikt untersagt.

Software für mehrere Umgebungen; Mehrsprachige Software; Dual-Medien-Software; Mehrere Kopien; Softwarebündel. Wenn Sie verschiedene Versionen der Software oder verschiedene Sprachausgaben der Software verwenden, wenn Sie die Software auf mehreren Medien erhalten, wenn Sie anderweitig mehrere Kopien der Software erhalten oder wenn Sie die Software mit einer anderen Software gebündelt erhalten sollten, entspricht die insgesamt zulässige Anzahl Ihrer Computer, auf denen alle Versionen der Software installiert sind, der Anzahl der Computer, die in den Lizenzen festgelegt ist, die Sie vom Rechtsinhaber bezogen haben, und jede erworbene Lizenz berechtigt Sie zur Installation und Nutzung der Software auf dieser Anzahl von Computern entsprechend den Festlegungen in den Klauseln 2.2 und 2.3, *außer die* Lizenzbedingungen sehen eine anderweitige Regelung vor.

2.2. Wenn die Software auf einem physischen Medium erworben wurde, haben Sie das Recht, die Software zum Schutz einer solchen Anzahl von Computern zu verwenden, die auf der Softwareverpackung festgelegt ist.
2.3. Wenn die Software über das Internet erworben wurde, haben Sie das Recht, die Software zum Schutz einer solchen Anzahl von Computern zu verwenden, die genannt wurde, als Sie die Lizenz für die Software erworben haben.
2.4. Sie haben das Recht, eine Kopie der Software anzufertigen, und zwar ausschließlich zu Sicherungszwecken und nur, um die rechtmäßig in Ihrem Besitz befindliche Kopie zu ersetzen, sollte eine solche Kopie verloren gehen, zerstört oder unbrauchbar werden. Diese Sicherungskopie kann nicht zu anderen Zwecken verwendet werden und muss zerstört werden, wenn Sie das Recht verlieren, die Software zu nutzen oder wenn Ihre Lizenz abläuft oder aus irgendeinem Grund im Einklang mit der gültigen Gesetzgebung im Land Ihres Wohnsitzes oder in dem Land, in dem Sie die Software nutzen, gekündigt werden sollte.
2.5. Sie können die nicht-exklusive Lizenz zur Nutzung der Software an andere Personen innerhalb des Rahmens der Ihnen vom Rechtsinhaber gewährten Lizenz übertragen, vorausgesetzt, dass der Empfänger allen Geschäftsbedingungen dieses Vertrags zustimmt bzw. bejaht, Sie vollständig in der vom Rechtsinhaber gewährten Lizenz zu vertreten. In dem Fall, dass Sie die vom Rechtsinhaber gewährten Rechte zur Nutzung der Software vollständig übertragen, müssen Sie alle Kopien der Software, und zwar einschließlich der Sicherungskopie, zerstören. Wenn Sie Empfänger einer übertragenen Lizenz sind, müssen Sie zustimmen, alle Geschäftsbedingungen dieses Vertrags einzuhalten. Wenn Sie den Geschäftsbedingungen dieses Vertrags nicht vollständig zustimmen, dürfen Sie die Software nicht installieren und/oder verwenden. Sie stimmen als Empfänger einer übertragenen Lizenz weiterhin zu, dass Sie über keine zusätzlichen oder besseren Rechte verfügen, als der ursprüngliche Endnutzer, der die Software vom Rechtsinhaber erworben hat.
2.6 Ab dem Zeitpunkt der Aktivierung der Software bzw. Installation der Lizenzschlüsseldatei (mit Ausnahme einer Testversion der Software) haben Sie das Recht, folgende Dienstleistungen für den auf der Softwareverpackung (falls Sie Software auf einem physischen Medium erworben haben) oder während des Erwerbs (falls die Software über das Internet erworben wurde) festgelegten Zeitraum zu beziehen:
- Updates der Software über das Internet, wenn und wie der Rechtsinhaber diese auf seiner Webseite oder mittels anderer Online-Dienste veröffentlicht. Jedwede Updates, die Sie erhalten, werden Teil der Software und die Geschäftsbedingungen dieses Vertrags gelten für diese;
- Technische Unterstützung über das Internet sowie technische Unterstützung über die Telefon-Hotline.

3. Aktivierung und Zeitraum
3.1. Falls Sie Modifikationen an Ihrem Computer oder an der darauf installierten Software anderer Anbieter vornehmen, kann der Rechtsinhaber von Ihnen verlangen, die Aktivierung der Software bzw. die Installation der Lizenzschlüsseldatei zu wiederholen. Der Rechtsinhaber behält sich das Recht vor, jegliche Mittel und Verifizierungsverfahren zu nutzen, um die Gültigkeit der Lizenz und/oder die Rechtmäßigkeit einer Kopie der Software, die auf Ihrem Computer installiert und/oder genutzt wird, zu verifizieren.
3.2. Falls die Software auf einem physischen Medium erworben wurde, kann die Software nach Ihrer Annahme dieses Vertrags mit Beginn ab dem Zeitpunkt der Annahme dieses Vertrags für die auf der Verpackung bezeichnete Periode genutzt werden.
3.3. Falls die Software über das Internet erworben wurde, kann die Software nach Ihrer Annahme dieses Vertrags für die während des Erwerbs bezeichnete Zeitdauer genutzt werden.
3.4. Sie haben das Recht, eine Testversion der Software zu nutzen, und zwar gemäß der Festlegung in Klausel 2.1 und ohne jedwede Gebühr für die einzelne geltende Evaluierungsperiode (30 Tage) ab dem Zeitpunkt der Aktivierung der Software im Einklang mit diesem Vertrag, *und zwar unter der Bedingung, dass*

die Testversion Ihnen nicht das Recht auf Updates und technische Unterstützung über das Internet und technische Unterstützung über die Telefon-Hotline einräumt. Wenn der Rechtsinhaber für die einzelne geltende Evaluierungsperiode einen anderen Zeitraum festlegt, erhalten Sie darüber eine Mitteilung.
3.5. Ihre Lizenz zur Nutzung der Software beschränkt sich auf den in den Klauseln 3.2 oder 3.3 (je nach Anwendbarkeit) bezeichneten Zeitraum. Die verbleibende Zeitdauer kann auf die im Benutzerhandbuch beschriebene Weise abgefragt werden.
3.6. Haben Sie die Software zur Nutzung auf mehr als einem Computer erworben, beginnt der Zeitraum, auf den Ihre Lizenz zur Nutzung der Software begrenzt ist, am Tag der Aktivierung der Software bzw. der Installation der Lizenzschlüsseldatei auf dem ersten Computer.
3.7. Unbeschadet anderer Rechtsmittel laut Gesetz oder Billigkeitsrecht, zu denen der Rechtsinhaber im Falle eines Verstoßes gegen die Geschäftsbedingungen dieses Vertrags durch Sie berechtigt ist, ist der Rechtsinhaber jederzeit, ohne Sie benachrichtigen zu müssen, dazu berechtigt, diese Lizenz zur Nutzung der Software zu kündigen, und zwar ohne den Verkaufspreis oder einen Teil davon zurückzuerstatten.
3.8. Sie stimmen zu, dass Sie bei der Nutzung der Software sowie bei der Verwendung jedweder Berichte oder Informationen, die sich als Ergebnis der Nutzung der Software ableiten, alle geltenden internationalen, nationalen, staatlichen, regionalen und lokalen Gesetze sowie gesetzlichen Bestimmungen, einschließlich (und ohne Beschränkung) Datenschutz-, Urheber-, Exportkontroll- und Verfassungsrecht, einhalten werden.
3.9. Außer wenn anderweitig hierin festgelegt, dürfen Sie keines der Rechte, die Ihnen unter diesem Vertrag gewährt werden, bzw. keine Ihrer hieraus entstehenden Pflichten übertragen oder abtreten.
3.10. Der Rechtsinhaber behält sich das Recht vor, die Möglichkeit zur Aktivierung der Software außerhalb der Region, in der sie vom Rechtsinhaber und/oder seinen Partnern erworben wurde, zu beschränken.
3.11. Wenn Sie die Software mit einem Aktivierungscode erworben haben, der gültig für eine Sprachversion der Software in der Region ist, in der sie vom Rechtsinhaber oder seinen Partnern erworben wurde, dann können Sie die Software nicht durch Anwendung eines Aktivierungscodes aktivieren, der für eine andere Sprachversion vorgesehen ist.
3.12. Im Falle von Beschränkungen, die unter den Punkten 3.10 und 3.11 spezifiziert werden, wird die entsprechende Information über diese Beschränkungen auf der Verpackung und/oder Internetseite des Rechtsinhabers und/oder seiner Partner angegeben.

4. Technische Unterstützung
4.1. Die in Klausel 2.6 dieses Vertrags erläuterte technische Unterstützung wird Ihnen gewährt, wenn das neueste Update der Software installiert wird (außer im Fall einer Testversion der Software).
Technischer Support: http://support.kaspersky.com

5. Sammeln von Informationen
5.1. Durch Zustimmung zu den Geschäftsbedingungen dieses Vertrags haben Sie eingewilligt, dem Rechtsinhaber Informationen über die ausführbaren Dateien und ihre Prüfsummen zur Verfügung zu stellen, um Ihr Sicherheits-Schutzniveau zu verbessern.
5.2. Um das Sicherheitsbewusstsein bezüglich neuer Bedrohungen und deren Quellen zu verbessern, bzw. um Ihr Sicherheits-Schutzniveau zu verbessern, ist der Rechtsinhaber ausdrücklich berechtigt, mit Ihrer Zustimmung, die ausdrücklich in der Kaspersky Security Network Datenerfassungserklärung bestätigt wurde, derartige Informationen zu empfangen. Sie können den Kaspersky Security Network Service während der Installation deaktivieren. Sie können ebenfalls jederzeit auf der Softwareoptionsseite den Kaspersky Security Network Service aktivieren und deaktivieren.
Sie bestätigen und erkennen weiterhin an, dass jedwede Informationen, die vom Rechtsinhaber erfasst werden, zum Zweck der Verfolgung und Veröffentlichung von Sicherheitsrisikotrends verwendet werden können, und zwar nach freiem Ermessen des Rechtsinhabers.
5.3. Die Software verarbeitet keine personenbezogenen Daten und kombiniert keine Verarbeitungsdaten und persönlichen Informationen.
5.4. Sollten Sie nicht wünschen, dass die von der Software gesammelten Informationen an den Rechtsinhaber geschickt werden, sollten Sie den Kaspersky Security Network Service nicht aktivieren und/oder deaktivieren.

6. Beschränkungen
6.1. Sie werden die Software nicht emulieren, klonen, vermieten, verleihen, leasen, verkaufen, modifizieren, dekompilieren oder zurückentwickeln oder disassemblieren oder Arbeiten auf Grundlage der Software oder eines Teils davon ableiten, jedoch mit der einzigen Ausnahme eines Ihnen durch geltende Gesetzgebung gewährten Rechts, von dem keine Rücktretung möglich ist, und Sie werden in keiner anderen Form irgendeinen Teil der Software in menschlich lesbare Form umwandeln oder die lizenzierte Software oder irgendeine Teilmenge der lizenzierten Software übertragen, noch irgendeiner Drittpartei gestatten, dies zu

tun, außer im Umfang vorangegangener Einschränkungen, die ausdrücklich durch geltendes Recht untersagt sind. Weder Binärcode noch Quellcode der Software dürfen verwendet oder zurückentwickelt werden, um den Programmalgorithmus, der proprietär ist, wiederherzustellen. Alle Rechte, die nicht ausdrücklich hierin gewährt werden, verbleiben beim Rechtsinhaber und/oder dessen Zulieferern, je nachdem, was zutrifft. Jegliche derartige nicht autorisierte Nutzung der Software kann zur sofortigen und automatischen Kündigung dieses Vertrags sowie der hierunter gewährten Lizenz und zu Ihrer straf- und/oder zivilrechtlichen Verfolgung führen.
6.2. Sie werden die Rechte zur Nutzung der Software nicht an eine Drittpartei übertragen, außer entsprechend der Festlegung in Klausel 2.5 dieses Vertrags.
6.3. Sie werden den Aktivierungscode und/oder die Lizenzschlüssel-Datei keinen Drittparteien verfügbar machen oder Drittparteien Zugang zum Aktivierungscode und/oder zum Lizenzschlüssel gewähren. Aktivierungscode und/oder Lizenzschlüssel werden/wird als vertrauliche Daten des Rechtsinhabers betrachtet, und Sie werden angemessene Sorgfalt zum Schutz der Vertraulichkeit des Aktivierungscodes und/oder des Lizenzschlüssels walten lassen, sofern Sie den Aktivierungscode und/oder den Lizenzschlüssel entsprechend der Festlegung in Klausel 2.5 dieses Vertrags an Drittparteien übertragen dürfen.
6.4. Sie werden die Software nicht an eine Drittpartei vermieten, verleasen oder verleihen.
6.5. Sie werden die Software nicht zur Erstellung von Daten oder Software verwenden, die zur Feststellung, zum Sperren oder zur Handhabung von Bedrohungen, wie im Nutzerhandbuch beschrieben, genutzt werden.
6.6. Der Rechtsinhaber hat das Recht, die Schlüsseldatei zu blockieren oder Ihre Lizenz zu kündigen, falls Sie gegen irgendwelche Geschäftsbedingungen dieses Vertrags verstoßen, und zwar ohne irgendeine Rückerstattung an Sie.
6.7. Falls Sie die Testversion der Software verwenden, sind Sie nicht berechtigt, technische Unterstützung, wie in Klausel 4 dieses Vertrags festgelegt, zu erhalten, und Sie sind ebenfalls nicht berechtigt, die Lizenz oder die Rechte zur Nutzung der Software an irgendeine Drittpartei zu übertragen.

7. Eingeschränkte Garantie und Haftungsausschluss
7.1. Der Rechtsinhaber garantiert, dass die Software im Wesentlichen im Einklang mit den im Nutzerhandbuch dargelegten Spezifikationen und Beschreibungen funktionieren wird, *jedoch vorausgesetzt,* dass eine solche eingeschränkte Garantie nicht für Folgendes gilt: (w) Mängel Ihres Computers und zugehörigen Verstoß, wofür der Rechtsinhaber ausdrücklich jedwede Gewährleistungsverantwortung ablehnt; (x) Funktionsstörungen, Defekte oder Ausfälle, resultierend aus falscher Verwendung, Missbrauch, Unfall, Nachlässigkeit, unsachgemäßer/m Installation, Betrieb oder Wartung, Diebstahl, Vandalismus, höherer Gewalt, terroristischen Akten, Stromausfällen oder -schwankungen, Unglück, Veränderung, nicht zulässiger Modifikation oder Reparaturen durch eine Partei außer dem Rechtsinhaber oder Maßnahmen einer sonstigen Drittpartei oder Aktionen ihrerseits, oder Ursachen außerhalb der Kontrolle des Rechtsinhabers; (y) jedweder Defekt, der dem Rechtsinhaber nicht durch Sie bekannt gemacht wird, sobald dies nach dem ersten Auftreten des Defekts möglich ist; und (z) Inkompatibilität, verursacht durch Hardware- und/oder Software-Komponenten, die auf Ihrem Computer installiert sind.
7.2. Sie bestätigen, akzeptieren und erkennen an, dass keine Software frei von Fehlern ist, und Sie sind angehalten, den Computer mit einer für Sie geeigneten Häufigkeit und Beständigkeit zu sichern.
7.3. Der Rechtsinhaber gibt keine Garantie, dass die Software im Fall von Verstößen gegen die Bedingungen, wie im Nutzerhandbuch oder in diesem Vertrag beschrieben, einwandfrei funktionieren wird.
7.4. Der Rechtsinhaber garantiert nicht, dass die Software einwandfrei funktionieren wird, wenn Sie nicht regelmäßig, wie in Klausel 2.6 dieses Vertrags erläutert, Updates herunterladen.
7.5. Der Rechtsinhaber garantiert keinen Schutz vor im Nutzerhandbuch beschriebenen Bedrohungen nach Ablauf der in Klausel 3.2 oder 3.3 dieses Vertrags bezeichneten Periode oder nachdem die Lizenz zur Nutzung der Software aus irgendeinem Grund gekündigt wurde.
7.6. DIE SOFTWARE WIRD OHNE MÄNGELGEWÄHR BEREITGESTELLT UND DER RECHTSINHABER GIBT KEINE ZUSICHERUNG UND KEINE GEWÄHRLEISTUNG IN BEZUG AUF IHRE NUTZUNG ODER LEISTUNG. DER RECHTSINHABER UND SEINE PARTNER GEWÄHREN AUßER DEN GARANTIEN, ZUSICHERUNGEN, BESTIMMUNGEN ODER BEDINGUNGEN, DIE DURCH GELTENDES RECHT NICHT AUSGESCHLOSSEN ODER BESCHRÄNKT WERDEN KÖNNEN, KEINE GARANTIEN, ZUSICHERUNGEN, BESTIMMUNGEN ODER BEDINGUNGEN (AUSDRÜCKLICHER ODER STILLSCHWEIGENDER NATUR, DIE ENTWEDER AUS EINER GESCHÄFTSBEZIEHUNG ODER EINEM HANDELSBRAUCH ENTSTEHEN BZW. AUS GESETZLICHEN, GEWOHNHEITSRECHTLICHTEN ODER ANDEREN VORSCHRIFTEN ABGELEITET WERDEN) HINSICHTLICH JEDWEDER ANGELEGENHEIT, EINSCHLIEßLICH (OHNE EINSCHRÄNKUNG) VON NICHTVERLETZUNG VON RECHTEN DRITTER, MARKTGÄNGIGKEIT, BEFRIEDIGENDE QUALITÄT, INTEGRIERUNG ODER BRAUCHBARKEIT FÜR

EINEN BESTIMMTEN ZWECK. SIE TRAGEN DAS GESAMTE STÖRUNGSRISIKO UND DAS GESAMTRISIKO HINSICHTLICH DER LEISTUNG UND VERANTWORTUNG FÜR DIE AUSWAHL DER SOFTWARE, UM IHRE VORGESEHENEN RESULTATE ZU ERZIELEN, UND FÜR DIE INSTALLATION SOWIE DIE NUTZUNG DER SOFTWARE UND DIE MIT IHR ERZIELTEN ERGEBNISSE. OHNE EINSCHRÄNKUNG DER VORANGEGANGENEN BESTIMMUNGEN MACHT DER RECHTSINHABER KEINE ZUSICHERUNGEN UND GIBT KEINE GEWÄHRLEISTUNG, DASS DIE SOFTWARE FEHLERFREI ODER FREI VON UNTERBRECHUNGEN ODER SONSTIGEN STÖRUNGEN IST ODER DASS DIE SOFTWARE JEDWEDE ODER ALL IHRE ANFORDERUNGEN ERFÜLLEN WIRD, UNGEACHTET DESSEN, OB GEGENÜBER DEM RECHTSINHABER OFFEN GELEGT ODER NICHT.

8. Haftungsausschluss und Haftungsbeschränkungen

8.1. INSOWEIT GESETZLICH STATTHAFT, SIND DER RECHTSINHABER UND SEINE PARTNER UNTER KEINEN UMSTÄNDEN HAFTBAR FÜR JEDWEDE SPEZIELLEN ODER BEILÄUFIGEN SCHÄDEN, STRAFZUSCHLAG ZUM SCHADENERSATZ, INDIREKTE ODER FOLGESCHÄDEN (EINSCHLIEßLICH UND NICHT BESCHRÄNKT AUF SCHÄDEN AUS VERLUST VON GEWINN ODER VERTRAULICHEN ODER SONSTIGEN INFORMATIONEN, FÜR GESCHÄFTSUNTERBRECHUNG, FÜR VERLUST VON PRIVATSPHÄRE, KORRUPTION, BESCHÄDIGUNG UND VERLUST VON DATEN ODER PROGRAMMEN, FÜR VERSÄUMNIS EINER PFLICHTERFÜLLUNG, EINSCHLIEßLICH JEDWEDER GESETZLICHER PFLICHTEN, TREUEPFLICHT ODER PFLICHT ZUR WAHRUNG ANGEMESSENER SORGFALT, FÜR NACHLÄSSIGKEIT, FÜR WIRTSCHAFTLICHEN VERLUST UND FÜR FINANZIELLEN ODER JEDWEDEN SONSTIGEN VERLUST), DIE AUS ODER AUF IRGENDEINE WEISE IM ZUSAMMENHANG MIT DER NUTZUNG ODER UNMÖGLICHKEIT DER NUTZUNG DER SOFTWARE, DER BEREITSTELLUNG ODER DEM VERSÄUMNIS DER BEREITSTELLUNG TECHNISCHER UNTERSTÜTZUNG ODER SONSTIGER DIENSTLEISTUNGEN, INFORMATIONEN, SOFTWARE UND ZUGEHÖRIGEM INHALT MITTELS DER SOFTWARE RESULTIEREN, ODER SICH ANDERWEITIG AUS DER NUTZUNG DER SOFTWARE ODER ANDERWEITIG UNTER BZW. IM ZUSAMMENHANG MIT EINER BESTIMMUNG DIESES VERTRAGS ERGEBEN, ODER DIE FOLGE EINES VERTRAGSBRUCHS ODER UNERLAUBTER HANDLUNG (EINSCHLIEßLICH NACHLÄSSIGKEIT, FALSCHANGABE, JEDWEDER STRIKTEN HAFTUNGSVERPFLICHTUNG ODER -PFLICHT), ODER EINER VERLETZUNG GESETZLICHER PFLICHTEN ODER DER GEWÄHRLEISTUNG DES RECHTSINHABERS ODER EINES SEINER PARTNER SIND, UND ZWAR AUCH DANN NICHT, WENN DER RECHTSINHABER ODER EINER SEINER PARTNER BEZÜGLICH DER MÖGLICHKEIT SOLCHER SCHÄDEN INFORMIERT WURDE.

SIE STIMMEN ZU, DASS IN DEM FALL, DASS DER RECHTSINHABER UND/ODER SEINE PARTNER HAFTBAR GEMACHT WERDEN/WIRD, DIE HAFTUNG DES RECHTSINHABERS UND/ODER SEINER PARTNER AUF DIE KOSTEN DER SOFTWARE BESCHRÄNKT IST. UNTER KEINEN UMSTÄNDEN WIRD DIE HAFTUNG DES RECHTSINHABERS UND/ODER SEINER PARTNER DIE FÜR DIE SOFTWARE ERSTATTETEN KOSTEN AN DEN RECHTSINHABER ODER DEN PARTNER ÜBERSTEIGEN (JE NACHDEM, WAS ZUTRIFFT).

NICHTS IN DIESEM VERTRAG SCHLIEßT EINEN ANSPRUCH AUFGRUND VON TOD UND PERSONENSCHADEN AUS ODER SCHRÄNKT DIESEN EIN. IN DEM FALL, DASS EIN HAFTUNGSAUSSCHLUSS, EIN AUSSCHLUSS ODER EINE EINSCHRÄNKUNG IN DIESEM VERTRAG AUFGRUND GELTENDEN RECHTS NICHT AUSGESCHLOSSEN ODER BESCHRÄNKT WERDEN KANN, WIRD NUR EIN SOLCHER HAFTUNGSAUSSCHLUSS, AUSSCHLUSS ODER EINE EINSCHRÄNKUNG NICHT FÜR SIE GELTEN, UND SIE SIND WEITERHIN AN JEDWEDE VERBLEIBENDEN HAFTUNGSAUSSCHLÜSSE, AUSSCHLÜSSE ODER EINSCHRÄNKUNGEN GEBUNDEN.

9. GNU und sonstige Drittpartei-Lizenzen

9.1. Die Software kann einige Softwareprogramme enthalten, die an den Nutzer unter der GPL (GNU General Public License) oder sonstigen vergleichbaren freien Softwarelizenzen lizenziert (oder unterlizenziert) sind und dem Nutzer neben anderen Rechten gestatten, bestimmte Programme oder Teile dieser Programme zu kopieren, zu modifizieren und weiter zu verbreiten und sich Zugang zum Quellcode zu verschaffen („Open Source Software“). Falls es solche Lizenzen erforderlich machen, dass für jedwede Software, die an jemanden in ausführbarem Binärformat geliefert wird, diesen Nutzern der Quellcode ebenfalls verfügbar gemacht wird, dann soll der Quellcode zur Verfügung gestellt werden, indem ein diesbezügliches Ersuchen an source@kaspersky.com gesendet wird, oder der Quellcode wird mit der Software geliefert. Falls irgendwelche Open Source Software-Lizenzen es erforderlich machen, dass der Rechtsinhaber Rechte zur Nutzung, zum Kopieren oder zur Änderung eines Open Source Software-Programms bereitstellt, welche umfassender sind, als die in diesem Vertrag gewährten Rechte, dann werden derartige Rechte Vorrang vor den hierin festgelegten Rechten und Einschränkungen haben.

10. Geistiges Eigentum

10.1. Sie stimmen zu, dass die Software sowie die Urheberschaft, Systeme, Ideen, Betriebsmethoden, Dokumentation und sonstige in der Software enthaltenen Informationen proprietäres geistiges Eigentum und/oder die wertvollen Geschäftsgeheimnisse des Rechtsinhabers oder seiner Partner sind und dass der Rechtsinhaber und seine Partner, je nachdem was zutrifft, durch das Zivil- und Strafrecht sowie durch Gesetze zum Urheberrecht, bezüglich Geschäftsgeheimnissen, Handelsmarken und Patenten der Russischen Föderation, der Europäischen Union und der Vereinigten Staaten sowie anderer Länder und internationaler Übereinkommen geschützt sind. Dieser Vertrag gewährt Ihnen keinerlei Rechte am geistigen Eigentum, einschließlich an jeglichen Handelsmarken und Servicemarken des Rechtsinhabers und/oder seiner Partner („Handelsmarken"). Sie dürfen die Handelsmarken nur so weit nutzen, um von der Software im Einklang mit der akzeptierten Handelsmarkenpraxis erstellte Druckausgaben zu identifizieren, einschließlich der Identifizierung des Namens des Besitzers der Handelsmarke. Eine solche Nutzung der Handelsmarke gibt Ihnen keinerlei Besitzrechte an dieser Handelsmarke. Der Rechtsinhaber und/oder seine Partner besitzen und behalten alle Rechte, Titel und Anteile an der Software, einschließlich (ohne jedwede Einschränkung) jedweden Fehlerkorrekturen, Erweiterungen, Updates oder sonstigen Modifikationen an der Software, ob durch den Rechtsinhaber oder eine beliebige Drittpartei vorgenommen, und allen Urheberrechten, Patenten, Rechten an Geschäftsgeheimnissen, Handelsmarken und sonstigem geistigen Eigentum daran. Ihr Besitz, die Installation oder Nutzung der Software lässt den Titel am geistigen Eigentum an der Software nicht auf Sie übergehen, und Sie erwerben keinerlei Rechte an der Software, außer jene ausdrücklich in diesem Vertrag dargelegten. Alle hierunter erstellten Kopien der Software müssen dieselben proprietären Informationen enthalten, die auf und in der Software erscheinen. Mit Ausnahme der hierin aufgeführten Bestimmungen gewährt Ihnen dieser Vertrag keine Rechte geistigen Eigentums an der Software und Sie bestätigen, dass diese unter diesem Vertrag gewährte Lizenz Ihnen gemäß den weiteren Festlegungen hierin ausschließlich das Recht auf eingeschränkte Nutzung unter den Geschäftsbedingungen dieses Vertrags gewährt. Der Rechtsinhaber behält sich alle Rechte vor, die Ihnen nicht ausdrücklich in diesem Vertrag gewährt wurden.

10.2. Sie stimmen zu, die Software in keinster Weise zu modifizieren oder abzuändern. Sie dürfen die Urheberrechtshinweise oder sonstige proprietäre Hinweise auf jedweden Kopien der Software nicht entfernen oder verändern.

11. Geltendes Recht; Schiedsverfahren

11.1. Dieser Vertrag unterliegt den Gesetzen der Russischen Föderation und wird nach diesen ausgelegt, und zwar ohne Bezug auf gegenteilige gesetzliche Regelungen und Prinzipien. Dieser Vertrag wird nicht dem Übereinkommen der Vereinten Nationen über Verträge über den internationalen Warenverkauf unterliegen, dessen Anwendung ausschließlich ausgeschlossen wird. Jede Meinungsverschiedenheit, die aus den Bedingungen dieses Vertrags, deren Auslegung oder Anwendung oder einem Verstoß gegen diese resultiert, wird, außer falls durch unmittelbare Verhandlung beigelegt, durch das Gericht der internationalen Handelsschiedsgerichtsbarkeit bei der Industrie- und Handelskammer der Russischen Föderation in Moskau, in der Russischen Föderation, beigelegt. Jeder vom Schlichter abgegebene Schiedsspruch ist für die beteiligten Parteien endgültig und bindend und jedwedes Urteil bezüglich eines solchen Schiedsspruchs kann von jedem Gericht der zuständigen Jurisdiktion durchgesetzt werden. Nichts in diesem Abschnitt 11 wird eine Partei daran hindern, von einem Gericht der zuständigen Jurisdiktion rechtmäßige Entschädigung zu verlangen oder zu erhalten, sei es vor, während oder nach einem Schiedsverfahren.

12. Zeitraum für Rechtsverfolgung

12.1. Von den Parteien dieses Vertrags kann keine Rechtsverfolgung, ungeachtet der Form, die sich aus Transaktionen unter diesem Vertrag ergibt, nach mehr als einem (1) Jahr nach dem Eintreten des Klagegrundes oder der Entdeckung dessen Eintritts ergriffen werden, außer, dass eine Rechtsverfolgung für Verletzung von Rechten geistigen Eigentums innerhalb des maximal geltenden gesetzlichen Zeitraums ergriffen wird.

13. Vollständigkeit der Vereinbarung, Salvatorische Klausel, kein Verzicht

13.1. Dieser Vertrag stellt die Gesamtvereinbarung zwischen Ihnen und dem Rechtsinhaber dar und ersetzt jegliche sonstigen, vorherigen Vereinbarungen, Vorschläge, Kommunikation oder Ankündigung, ob mündlich oder schriftlich, in Bezug auf die Software oder den Gegenstand dieser Vereinbarung. Sie bestätigen, dass Sie diesen Vertrag gelesen haben, ihn verstehen und seinen Bedingungen zustimmen. Falls eine Bestimmung dieses Vertrags von einem Gericht der zuständigen Jurisdiktion insgesamt oder in Teilen als untauglich, ungültig oder aus welchen Gründen auch immer als nicht durchsetzbar angesehen wird, wird diese Bestimmung enger ausgelegt, damit sie rechtmäßig und durchsetzbar wird, und der Gesamtvertrag

wird an diesem Umstand nicht scheitern, und die Ausgewogenheit des Vertrags bleibt weiterhin vollinhaltlich gültig und wirksam, so weit gesetzlich oder nach Billigkeitsrecht zulässig, während der ursprüngliche Inhalt weitest möglich beibehalten wird. Kein Verzicht auf eine hierin enthaltene Bestimmung oder Kondition ist gültig, außer in schriftlicher Form und durch Sie und einen autorisierten Vertreter des Rechtsinhabers unterzeichnet, vorausgesetzt, dass kein Verzicht einer Verletzung einer Bestimmung dieses Vertrags einen Verzicht eines vorherigen, gleichzeitigen oder Folgeverstoßes konstituiert. Nichtverfolgung oder fehlende Durchsetzung einer Bestimmung dieses Vertrags durch den Rechtsinhaber kann nicht als Verzicht auf diese Bestimmung oder dieses Recht geltend gemacht werden.

14. Kontaktinformationen des Rechtsinhabers

Sollten Sie Fragen in Bezug auf diesen Vertrag haben oder sollten Sie wünschen, sich aus irgendeinem Grund mit dem Rechtsinhaber in Verbindung zu setzen, kontaktieren Sie bitte unsere Kundendienstabteilung unter:
Kaspersky Lab ZAO, 10 build. 1, 1st Volokolamsky Proezd
Moskau, 123060
Russische Föderation
Tel.: +7-495-797-8700
Fax: +7-495-645-7939
E-Mail: info@kaspersky.com
Webseite: http://www.kaspersky.com

© 1997-2010 Kaspersky Lab ZAO. Alle Rechte vorbehalten. Die Software und jedwede begleitende Dokumentation unterliegen dem Urheberrecht bzw. dem Schutz durch Urheberrechtsgesetze und internationale Urheberrechtsabkommen sowie durch weitere Gesetze und Abkommen zum geistigen Eigentum.

ÜBER DIESES HANDBUCH

Dieses Handbuch informiert über Installation, Konfiguration und Verwendung des Programms Kaspersky PURE 9.1 (im Folgenden Kaspersky PURE genannt). Das Dokument ist für gewöhnliche Anwender gedacht. Zur Verwendung des Programms sind Grundkenntnisse im Umgang mit einem PC erforderlich: Der Anwender sollte das Interface und die Funktionen des Betriebssystems Microsoft Windows auf grundlegendem Niveau beherrschen sowie gängige E-Mail-Programme und Browser wie Microsoft Office Outlook und Microsoft Internet Explorer bedienen können.

Das Dokument soll:

- dem Anwender helfen, das Programm selbst auf einem Computer zu installieren, es zu aktivieren und unter Berücksichtigung individueller Aufgaben optimal anzupassen.
- Fragen, die sich auf das Programm beziehen, schnell beantworten.
- auf alternative Informationsquellen über das Programm und auf Möglichkeiten des technischen Supports hinweisen.

IN DIESEM ABSCHNITT

In diesem Dokument 19

Formatierung mit besonderer Bedeutung 20

IN DIESEM DOKUMENT

Das Benutzerhandbuch für Kaspersky PURE besteht aus folgenden Kapiteln:

Zusätzliche Informationsquellen

Dieser Abschnitt enthält eine Beschreibung der Quellen, die zusätzliche Informationen über das Programm bieten, und verweist auf Internetressourcen, die zur Diskussion über das Programm, für Vorschläge, sowie für Fragen und Antworten dienen.

Kaspersky PURE

Dieser Abschnitt enthält eine Beschreibung der Möglichkeiten der Anwendung und sowie über seine Komponenten und Grundfunktionen. Hier können Sie mehr über den Lieferumfang und die Services erfahren, die den registrierten Programmnutzern zur Verfügung stehen. Außerdem werden die Hard- und Softwarevoraussetzungen genannt, denen ein Computer entsprechen muss, damit Kaspersky PURE darauf installiert werden kann.

Installation auf einem Computer

Dieser Abschnitt enthält Anleitungen, die dem Anwender helfen, das Programm auf einem Computer zu installieren oder eine Vorgängerversion zu aktualisieren. Dieser Abschnitt beschreibt, wie das Programm von einem Computer deinstalliert wird.

Lizenzverwaltung

Dieser Abschnitt informiert über die wichtigsten Begriffe, die mit der Programmlizenzierung zusammenhängen. In diesem Abschnitt erfahren Sie außerdem, wie die Gültigkeitsdauer für eine Lizenz automatisch verlängert werden kann und wo sich Informationen zur aktiven Lizenz befinden.

Programmoberfläche

Dieser Abschnitt beschreibt die wichtigsten Elemente der grafischen Programmoberfläche: Symbol und Kontextmenü des Programms, Hauptfenster, Konfigurationsfenster und Meldungsfenster.

Programm starten und beenden

Dieser Abschnitt informiert darüber, wie das Programm gestartet und beendet wird.

Schutzstatus des Computers

Dieser Abschnitt informiert darüber, wie ermittelt wird, ob der Computer im Augenblick sicher ist oder ob seine Sicherheit bedroht ist. Außerdem wird die Neutralisierung von vorhandenen Bedrohungen beschrieben. Hier finden Sie Informationen darüber, wie der Schutz während der Arbeit von Kaspersky PURE aktiviert, deaktiviert und vorübergehend angehalten werden kann.

Lösungen für typische Aufgaben

Dieser Abschnitt bietet eine Anleitung für die grundlegenden Aufgaben des Programms, die der Benutzer am häufigsten benötigt.

Erweiterte Programmeinstellungen

Dieser Abschnitt beschreibt die einzelnen Komponenten und informiert über ihre Einstellungen für einen flexiblen und effektiven Schutz.

Überprüfung der Programmeinstellungen

Dieser Abschnitt enthält Tipps zur Überprüfung der Einstellungen für die Programmkomponenten.

Kontaktaufnahme mit dem Technischen Support

Dieser Abschnitt enthält Tipps dazu, wie Sie auf der Support-Webseite aus Mein Kaspersky Account oder telefonisch Hilfe von Kaspersky Lab erhalten können.

Anhänge

Dieser Abschnitt enthält Hilfeinformationen, die den Haupttext des Dokuments ergänzen.

Glossar

Dieser Abschnitt enthält eine Liste und Definitionen der Begriffe, die in diesem Dokument vorkommen.

FORMATIERUNG MIT BESONDERER BEDEUTUNG

Die Bedeutung der in diesem Dokument verwendeten Textformatierungen wird in folgender Tabelle erläutert.

Tabelle 1. Formatierung mit besonderer Bedeutung

TEXTBEISPIEL	BESCHREIBUNG DER FORMATIERUNG
Beachten Sie, dass ...	Warnungen sind rot geschrieben und eingerahmt. Warnungen enthalten wichtige Informationen, die z.B. auf Aktionen hinweisen, die im Hinblick auf die Computersicherheit als kritisch gelten.

TEXTBEISPIEL	BESCHREIBUNG DER FORMATIERUNG
Es wird empfohlen,...	Hinweise sind eingerahmt. Hinweise enthalten hilfreiche und informative Angaben.
Beispiel: ...	Beispiele sind gelb unterlegt und mit "Beispiel" überschrieben.
Das *Update* ist...	Neue Begriffe sind kursiv geschrieben.
ALT+F4	Bezeichnungen von Tasten sind halbfett und in Großbuchstaben geschrieben. Tastenbezeichnungen, die mit einem Pluszeichen verbunden sind, bedeuten eine Tastenkombination.
Aktivieren	Die Namen von Elementen der Benutzeroberfläche (z.B. Eingabefelder, Menübefehle, Schaltflächen) sind halbfett geschrieben.
➧ *Gehen Sie folgendermaßen vor, um den Aufgabenzeitplan anzupassen:*	Der erste Satz einer Anleitung ist kursiv geschrieben.
`help`	Texte in der Befehlszeile oder Meldungstexte, die das Programm auf dem Bildschirm anzeigt, werden durch spezielle Schrift hervorgehoben.
<IP-Adresse Ihres Computers>	Variable stehen in eckigen Klammern. Eine Variable muss in einem konkreten Fall durch einen entsprechenden Wert ersetzt werden. Dabei fallen die eckigen Klammern weg.

ZUSÄTZLICHE INFORMATIONSQUELLEN

Fragen zu Auswahl, Kauf, Installation oder Verwendung von Kaspersky PURE haben, lassen sich unter Verwendung unterschiedlicher Informationsquellen beantworten. Sie können abhängig von der Dringlichkeit und Bedeutung Ihrer Frage eine passende Quelle wählen.

IN DIESEM ABSCHNITT

Informationsquellen zur selbständigen Recherche 22

Diskussion über die Programme von Kaspersky Lab im Webforum 23

Kontaktaufnahme mit der Vertriebsabteilung 23

Kontakt zur Abteilung für Handbücher und Hilfesysteme 23

INFORMATIONSQUELLEN ZUR SELBSTÄNDIGEN RECHERCHE

Kaspersky Lab bietet folgende Informationsquellen zu dem Programm an:

- Seite über das Programm auf der Webseite von Kaspersky Lab
- Seite über das Programm auf der Webseite des Technischen Supports (in der Wissensdatenbank)
- Seite des Interaktiven Supports
- Elektronisches Hilfesystem

Seite auf der Webseite von Kaspersky Lab

Auf dieser Seite (http://www.kaspersky.com/de/kaspersky-pure) finden Sie allgemeine Informationen über das Programm, seine Funktionen und Besonderheiten.

Seite auf der Webseite des Technischen Supports (Wissensdatenbank)

Auf dieser Seite (http://support.kaspersky.com/de/pure) finden Sie Artikel, die von Spezialisten des technischen Supports veröffentlicht wurden.

Diese Artikel bieten nützliche Informationen, Tipps und Antworten auf häufige Fragen zu Kauf, Installation und Verwendung vom Programm. Sie sind nach Themen wie "Mit der Produktlizenz arbeiten", "Update anpassen" oder "Störungen bei der Arbeit beheben" angeordnet. Die Artikel können auch Fragen behandeln, die neben diesem Programm auch andere Produkte von Kaspersky Lab betreffen. Außerdem können sie allgemeine Neuigkeiten über den Technischen Support enthalten.

Interaktiver Support

Auf der Seite dieses Dienstes finden Sie eine regelmäßig aktualisierte Datenbank mit häufig auftretenden Fragen und Antworten über die Arbeit des Programms. Um diesen Dienst nutzen zu können, ist eine Internetverbindung erforderlich.

- Um zur Serviceseite zu wechseln, verwenden Sie im Programmhauptfenster den Link **Support** und klicken Sie im folgenden Fenster auf **Interaktiver Support**.

Elektronisches Hilfesystem

Im Lieferumfang des Programms ist eine vollständige und kontextorientierte Hilfedatei enthalten. Sie bietet Informationen zu folgenden Aspekten des Computerschutzes: Anzeige des Schutzstatus, Untersuchung bestimmter Computerbereiche auf Viren, Ausführen anderer Aufgaben. Außerdem bietet die vollständige und kontextorientierte Hilfedatei Informationen zu jedem Programmfenster: verfügbare Parameter und deren Beschreibung sowie eine Liste mit den auszuführenden Aufgaben.

Um die Hilfe zu öffnen, klicken Sie im entsprechenden Fenster auf **Hilfe** oder auf die Taste **F1**.

DISKUSSION ÜBER DIE PROGRAMME VON KASPERSKY LAB IM WEBFORUM

Wenn Ihre Frage keine dringende Antwort erfordert, können Sie sie mit den Spezialisten von Kaspersky Lab und mit anderen Anwendern in unserem Forum unter der Adresse http://forum.kaspersky.com diskutieren.

Im Forum können Sie bereits veröffentlichte Themen nachlesen, eigene Beiträge schreiben, neue Themen eröffnen und die Hilfefunktion verwenden.

KONTAKTAUFNAHME MIT DER VERTRIEBSABTEILUNG

Bei Fragen zur Auswahl oder zum Kauf von der Kaspersky Produkte sowie zur Verlängerung der Nutzungsdauer stehen Ihnen die Mitarbeiter der Vertriebsabteilung in Deutschland unter folgenden Rufnummern zur Verfügung:

+49 (0) 841 – 981 89 560

Die Beratung erfolgt auf Deutsch oder Englisch.

Sie können sich mit Ihrer Frage auch über unser Kontaktformular an die Mitarbeiter der Vertriebsabteilung wenden.

KONTAKT ZUR ABTEILUNG FÜR HANDBÜCHER UND HILFESYSTEME

Wenn Sie Fragen zu dieser Dokumentation haben, einen Fehler darin gefunden haben oder Ihre Meinung über unsere Dokumentationen schreiben möchten, richten Sie sich bitte direkt an unsere Abteilung für Handbücher und Hilfesysteme. Zur Kontaktaufnahme mit der Dokumentationsgruppe senden Sie eine Nachricht an docfeedback@kaspersky.de. Geben Sie folgenden Betreff an: "Kaspersky Help Feedback: Kaspersky PURE".

KASPERSKY PURE

Dieser Abschnitt enthält eine Beschreibung der Möglichkeiten der Anwendung und sowie über seine Komponenten und Grundfunktionen. Hier können Sie mehr über den Lieferumfang und die Services erfahren, die den registrierten Programmnutzern zur Verfügung stehen. Außerdem werden die Hard- und Softwarevoraussetzungen genannt, denen ein Computer entsprechen muss, damit Kaspersky PURE darauf installiert werden kann.

IN DIESEM ABSCHNITT

Lieferumfang 24

Organisation des Schutzes für ein Heimnetzwerk 25

Service für registrierte Benutzer 27

Hard- und Softwarevoraussetzungen 28

LIEFERUMFANG

Kaspersky PURE kann bei unseren Vertriebspartnern (als verpackte Variante) oder in einem Online-Shop (z.B. http://www.kaspersky.com/de, Abschnitt **E-Store**) erworben werden.

Wurde das Programm in einer CD-Box erworben, gehören zum Lieferumfang des Programms:

- Versiegelter Umschlag mit Installations-CD, auf der die Programmdateien und die Dokumentation im PDF-Format gespeichert sind.
- Dokumentation in ausgedruckter Form, dieses Benutzerhandbuch und eine Quick-Start-Anleitung.
- Lizenzvereinbarung (je nach Region).
- Aktivierungskarte mit Aktivierungscode und Anleitung zur Aktivierung des Programms (je nach Region).

Die Lizenzvereinbarung ist ein juristischer Vertrag zwischen Ihnen und Kaspersky Lab, in dem steht, unter welchen Bedingungen Sie das von Ihnen gekaufte Programm gebrauchen dürfen.

Lesen Sie sich die Lizenzvereinbarung genau durch!

Wenn Sie die Bedingungen der Lizenzvereinbarung nicht annehmen, können Sie die Box an den Fachhändler zurückgeben, bei dem Sie sie gekauft haben, und Sie bekommen Ihr Geld zurück. Der Umschlag mit der Installations-CD (oder Disketten) muss noch versiegelt sein.

Wenn Sie den versiegelten Umschlag mit der Installations-CD (oder den Disketten) öffnen, nehmen Sie dadurch alle Bedingungen in der Lizenzvereinbarung an.

Bevor Sie den Umschlag mit der CD (oder den Disketten) aufbrechen, lesen Sie sich bitte die Lizenzvereinbarung sorgfältig durch.

Beim Erwerb von Kaspersky PURE in einem Online-Shop kopieren Sie das Produkt von der Kaspersky-Lab-Internetseite. Die Distribution enthält neben dem eigentlichen Produkt auch die vorliegende Dokumentation. Der Aktivierungscode wird Ihnen per E-Mail nach Eingang des Rechnungsbetrages zugestellt.

ORGANISATION DES SCHUTZES FÜR EIN HEIMNETZWERK

Kaspersky PURE bietet Ihrem Heimnetzwerk einen komplexen Schutz. Der Begriff Komplexer Schutz umfasst den Schutz des Computers, der Daten und der Benutzer. Außerdem bezieht er sich auf die Fernverwaltung der Funktionen von Kaspersky PURE auf allen Netzwerkcomputern.

In Kaspersky PURE sind unterschiedliche Funktionsmodule für die einzelnen Aufgaben des komplexen Schutzes verantwortlich.

Computersicherheit

Die *Schutzkomponenten* schützen Ihrem Computer vor bekannten und neuen Bedrohungen, Netzwerkangriffen und Betrugsversuchen, Spam und anderen unerwünschten Informationen. Jeder Bedrohungstyp wird von einer speziellen Schutzkomponente verarbeitet (s. Beschreibung der Komponenten weiter unten in diesem Abschnitt). Die Komponenten können unabhängig voneinander aktiviert und deaktiviert werden und lassen sich flexibel anpassen.

Zusätzlich zum Echtzeitschutz, den die Schutzkomponenten realisieren, wird eine regelmäßige *Untersuchung* Ihres Computers empfohlen. Das ist erforderlich, um die Möglichkeit der Ausbreitung schädlicher Programme auszuschließen, die nicht von den Schutzkomponenten erkannt wurden, weil beispielsweise eine zu niedrige Schutzstufe eingestellt war.

Um Kaspersky PURE auf dem neuesten Stand zu halten, ist ein *Update* der Datenbanken und Programm-Module erforderlich, die bei der Arbeit des Programms verwendet werden.

Programme, an deren Sicherheit Sie zweifeln, können in der speziellen *Sicheren Umgebung* gestartet werden.

Einige spezifische Aufgaben, die nicht regelmäßig, sondern nur gelegentlich anfallen, werden mit Hilfe *zusätzlicher Tools und Assistenten* ausgeführt. Dazu zählen beispielsweise die Konfiguration des Browsers Microsoft Internet Explorer oder das Löschen von Aktivitätsspuren des Benutzers im System.

Der Echtzeitschutz Ihres Computers wird durch folgende Schutzkomponenten gewährleistet:

Datei-Anti-Virus

> Datei-Anti-Virus erlaubt es, das Dateisystem des Computers vor einer Infektion zu schützen. Die Komponente wird beim Hochfahren des Betriebssystems gestartet, befindet sich ständig im Arbeitsspeicher des Computers und untersucht alle Dateien, die auf Ihrem Computer und auf allen angeschlossenen Laufwerken geöffnet, gespeichert und gestartet werden. Kaspersky PURE fängt jeden Zugriff auf eine Datei ab und untersucht die Datei nach bekannten Viren. Eine Datei wird nur dann zur Arbeit freigegeben, wenn die Datei virenfrei ist oder erfolgreich vom Programm desinfiziert wurde. Wenn die Desinfektion einer Datei nicht möglich ist, wird sie gelöscht. Dabei wird eine Kopie der Datei im Backup abgelegt oder in der Quarantäne gespeichert.

Mail-Anti-Virus

> Mail-Anti-Virus untersucht ein- und ausgehende E-Mails auf Ihrem Computer. Eine E-Mail wird nur dann dem Empfänger zugestellt, wenn sie keine gefährlichen Objekte enthält.

Web-Anti-Virus

> Web-Anti-Virus fängt die Ausführung von Skripts, die sich auf Webseiten befinden, ab und blockiert sie, falls Sie gefährlich sind. Auch der gesamte Web-Datenverkehr unterliegt der Kontrolle. Außerdem blockiert die Komponente den Zugriff auf gefährliche Webseiten.

IM-Anti-Virus

> IM-Anti-Virus sorgt für die Sicherheit bei Instant-Messengern. Die Komponente schützt die Informationen, die über Instant-Messenger-Protokolle auf Ihren Computer gelangen. IM-Anti-Virus gewährleistet Sicherheit bei der Arbeit mit vielen Programmen, die dem Sofortaustausch von Nachrichten dienen.

Proaktiver Schutz

Der Proaktive Schutz erlaubt es, ein neues Schadprogramm zu erkennen, bevor es Schaden anrichten kann. Die Arbeit der Komponente basiert auf der Kontrolle und Analyse des Verhaltens aller auf Ihrem Computer installierten Programme. Abhängig von den auszuführenden Aktionen entscheidet Kaspersky PURE, ob ein Programm potentiell gefährlich ist. So ist Ihr Computer nicht nur vor bekannten Viren, sondern auch vor neuen, bisher unbekannten Viren geschützt.

Programmkontrolle

Programmkontrolle registriert die Aktionen, die von Programmen im System ausgeführt werden können, und reguliert in Abhängigkeit von der Gruppe, zu der ein Programm gehört, seine Aktivität. Für jede Gruppe von Programmen ist eine Auswahl von Regeln vorgegeben. Diese Regeln steuern den Zugriff von Programmen auf unterschiedliche Ressourcen des Betriebssystems.

Firewall

Firewall gewährleistet Sicherheit bei der in lokalen Netzwerken und im Internet. Die Komponente führt die Filterung der gesamten Netzwerkaktivität durch, wozu zwei Arten von Regeln dienen: *Regeln für Programme* und *Paketregeln*.

Netzwerkmonitor

Diese Komponente dient dazu, in Echtzeit Informationen über die Netzwerkaktivität anzuzeigen.

Schutz vor Netzwerkangriffen

Der Schutz vor Netzwerkangriffen wird beim *Hochfahren des Betriebssystems gestartet und überwacht den eingehenden Datenverkehr auf für Netzwerkangriffe charakteristische Aktivität. Wenn ein Angriffsversuch auf den Computer erkannt wird, blockiert Kaspersky PURE jede Art von Netzwerkaktivität des angreifenden Computers im Hinblick auf Ihrem Computer.*

Anti-Spam

Anti-Spam wird in Ihr Mailprogramm integriert und kontrolliert alle eingehenden E-Mail auf Spam. Alle E-Mails, die Spam enthalten, werden durch eine spezielle Kopfzeile markiert. Anti-Spam kann zusätzlich für die Spam-Verarbeitung (automatisches Löschen, Verschieben in einen speziellen Ordner, u.a.) eingestellt werden.

Anti-Phishing

Komponente, die in Web-Anti-Virus, Anti-Spam und IM-Anti-Virus integriert ist und mit der Webadressen auf ihre Zugehörigkeit zur Liste der Phishing- und verdächtigen Webadressen untersucht werden können.

Anti-Banner

Anti-Banner blockiert Werbung, die auf speziellen Bannern platziert ist, die in das Interface von auf Ihrem Computer installierten Programmen integriert sind oder sich im Internet befinden.

Informationsschutz

Die Funktionen Backup, Datenverschlüsselung und Password Manager schützen die Daten vor Verlust, unbefugtem Zugriff und Diebstahl.

Backup

Es gibt unterschiedliche Gründe für den Verlust oder die Beschädigung von Daten auf einem Computer: beispielsweise eine Vireninfektion, Veränderungen oder das Löschen von Informationen durch andere Benutzer u.a. Um den Verlust wichtiger Daten zu vermeiden, ist eine regelmäßige Datensicherung unerlässlich.

Mit der Backup-Funktion lassen sich auf einem ausgewählten Datenträger in einem speziellen Speicher Sicherungskopien von Daten anlegen. Zu diesem Zweck werden Update-Aufgaben erstellt. Eine Aufgabe kann entweder manuell oder automatisch nach Zeitplan gestartet werden und dient dazu, in einem Speicher Sicherungskopien ausgewählter Dateien anzulegen. Bei Bedarf kann eine gespeicherte Datei in der erforderlichen

Version aus einer Sicherungskopie wiederhergestellt werden. Dadurch bietet ein regelmäßiges Backup zusätzliche Sicherheit für die Daten.

Datenverschlüsselung

Vertrauliche Informationen, die in elektronischer Form gespeichert sind, erfordern einen zusätzlichen Schutz vor unbefugtem Zugriff. Dazu dient die Speicherung der Daten in einem verschlüsselten Container.

Die Datenverschlüsselung erlaubt es, auf einem ausgewählten Datenträger verschlüsselte Spezialcontainer zu erstellen. Diese Container werden im System als virtuelle Wechseldatenträger dargestellt. Für den Zugriff auf die Daten, die in einem verschlüsselten Container gespeichert sind, ist aber die Eingabe des Kennworts erforderlich.

Password Manager

Der Zugriff auf eine Vielzahl von Diensten und Ressourcen erfolgt heutzutage durch die Anmeldung des Benutzers und die anschließende Eingabe von Benutzerdaten zum Zweck der Authentifizierung. Aus Sicherheitsgründen wird davor gewarnt, für unterschiedliche Ressourcen identische Benutzerdaten zu verwenden und sich Benutzername und Kennwort aufzuschreiben. Es ist schwierig, sich eine große Anzahl von Benutzerdaten einzuprägen. Dadurch gewinnt das Problem einer sicheren Speicherung von Kennwörtern an Aktualität.

Der Password Manager kann unterschiedliche Arten persönlicher Daten (z.B. Benutzernamen, Kennwörter, Adressen, Telefon- und Kreditkartennummern) in verschlüsselter Form speichern. Der Zugriff auf die Daten wird durch ein einziges Master-Kennwort geschützt. Nach Eingabe des Master-Kennworts erlaubt der Password Manager es, die Felder unterschiedlicher Authentifizierungsformulare automatisch auszufüllen. Es ist also ausreichend, sich nur ein einziges Master-Kennwort zu merken, um alle Benutzerdaten zu verwalten.

Kindersicherung

Die Funktionen der Kindersicherung dienen dazu, Kinder und Jugendliche vor Gefahren zu schützen, die bei der Arbeit am Computer und im Internet bestehen.

Die Kindersicherung erlaubt es, den Zugriff auf Internetressourcen und Programme für unterschiedliche Computerbenutzer altersabhängig flexibel einzuschränken. Außerdem erlaubt es diese Funktion, Berichte mit einer Statistik über die Aktionen der kontrollierten Benutzer anzuzeigen:

Verwaltung

Die Sicherheitsverwaltung eines lokalen Netzwerks wird erschwert, weil es aus mehreren Computer besteht. Schwachstellen, die zunächst nur einen Computer betreffen, können schnell das gesamte Netzwerk bedrohen.

Die Verwaltung bietet folgende Funktionen: netzwerkweite Untersuchungsaufgabe oder Updateaufgabe starten, Datensicherung verwalten, von einem lokalen Computer aus die Kindersicherung für alle Netzwerkcomputer anpassen. Dadurch lässt sich die Sicherheit für alle Computer, die zu einem lokalen Netzwerk gehören, fernverwalten.

SERVICE FÜR REGISTRIERTE BENUTZER

Kaspersky Lab ZAO bietet den legalen Benutzern ein umfangreiches Spektrum an Leistungen an, die den wirkungsvollen Einsatz des Programms effektiver gestalten.

Durch den Kauf einer Lizenz werden Sie zum registrierten Benutzer und können während der Gültigkeitsdauer der Lizenz folgende Leistungen in Anspruch nehmen:

- Stündliches Update der Programm-Datenbanken und Upgrade auf neue Programmversionen.
- Beratung bei Fragen zur Installation, Konfiguration und Nutzung des Programms per Telefon und über Mein Kaspersky Account.
- Benachrichtigung über das Erscheinen neuer Kaspersky-Lab-Programme und über neue Viren. Dieser Service wird Benutzern geboten, die den Newsletter von Kaspersky Lab auf (http://www.kaspersky.de/lab-news) abonniert haben.

Die Beratung bezieht sich nicht auf Fragen zu Funktion und Gebrauch von Betriebssystemen, Software von Drittherstellern und Funktionsweise verschiedener Technologien.

HARD- UND SOFTWAREVORAUSSETZUNGEN

Um die normale Funktionsfähigkeit von Kaspersky PURE zu gewährleisten, sind folgende Systemvoraussetzungen zu erfüllen:

Allgemeine Anforderungen:

- 500 MB freier Speicherplatz auf der Festplatte.
- CD-ROM-Laufwerk (für Installation von Kaspersky PURE von Installations-CD).
- Microsoft Internet Explorer 6.0 oder höher (für Update der Datenbanken und Programm-Module über das Internet).
- Microsoft Windows Installer 2.0.
- Maus.
- Internetverbindung für die Aktivierung von Kaspersky PURE.

Microsoft Windows XP Home Edition (Service Pack 3), Microsoft Windows XP Professional (Service Pack 3), Microsoft Windows XP Professional x64 Edition (Service Pack 3)*:*

- Intel Pentium 300 MHz oder höher (oder kompatibel).
- 256 MB Arbeitsspeicher.

Microsoft Windows Vista Home Basic (32-bit/64-bit, Service Pack 2), Microsoft Windows Vista Home Premium (32-bit/64-bit, Service Pack 2), Microsoft Windows Vista Business (32-bit/64-bit, Service Pack 2), Microsoft Windows Vista Enterprise (32-bit/64-bit, Service Pack 2), Microsoft Windows Vista Ultimate (32-bit/64-bit, Service Pack 2):

- Prozessor Intel Pentium 1 MHz 32-bit (x86)/ 64-bit (x64) oder höher (oder ein entsprechender kompatibler Prozessor.
- 1 GB Arbeitsspeicher.

Microsoft Windows 7 Home Premium, Microsoft Windows 7 Professional, Microsoft Windows 7 Ultimate:

- Prozessor Intel Pentium 1 MHz 32-bit (x86)/ 64-bit (x64) oder höher (oder ein entsprechender kompatibler Prozessor.
- 1 GB Arbeitsspeicher (32-Bit); 2 GB Arbeitsspeicher (64-Bit).

PROGRAMM INSTALLIEREN UND DEINSTALLIEREN

Dieser Abschnitt enthält Anleitungen, die dem Anwender helfen, das Programm auf einem Computer zu installieren oder eine Vorgängerversion zu aktualisieren. Dieser Abschnitt beschreibt, wie das Programm von einem Computer deinstalliert wird.

IN DIESEM ABSCHNITT

Installation des Programms auf einem Computer 30

Programm mit Hilfe des Installationsassistenten ändern, reparieren oder löschen 40

INSTALLATION DES PROGRAMMS AUF EINEM COMPUTER

Kaspersky PURE wird auf dem Computer interaktiv mit einem Installationsassistenten installiert.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**. Zum Abschluss des Assistenten dient die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf **Abbrechen** abgebrochen werden.

Vor der Installation sollten Sie alle laufenden Programme schließen.

- *Um Kaspersky PURE auf Ihrem Computer zu installieren,*

  starten Sie auf der Produkt-CD die Installationsdatei (Datei mit der Erweiterung .exe).

Wenn Kaspersky PURE über das Internet bezogen wurde, entspricht der Installationsvorgang für das Programm der Installation von CD-ROM.

IN DIESEM ABSCHNITT

Schritt 1. Nach neuer Programmversion suchen 31

Schritt 2. Systemkompatibilität für Installation prüfen 32

Schritt 3. Installationstyp auswählen 32

Schritt 4. Lizenzvereinbarung anzeigen 32

Schritt 5. Erklärung zur Verwendung von Kaspersky Security Network 32

Schritt 6. Zielordner auswählen 33

Schritt 7. Programmkomponenten für Installation auswählen 33

Schritt 8. Nach anderen Antiviren-Anwendungen suchen 34

Schritt 9. Firewall von Microsoft Windows deaktivieren 34

Schritt 10. Installation vorbereiten 34

Schritt 11. Installation 35

Schritt 12. Programm aktivieren 35

Schritt 13. Daten überprüfen 35

Schritt 14. Anmeldung des Benutzers 35

Schritt 15. Aktivierung abschließen 36

Schritt 16. Kontrolle des Zugriffs auf das Programm 36

Schritt 17. Schutzmodus auswählen 36

Schritt 18. Programm-Update anpassen 37

Schritt 19. Erkennbare Bedrohungen auswählen 37

Schritt 20. Systemanalyse 38

Schritt 21. Assistent abschließen 38

Erste Schritte 39

SCHRITT 1. NACH NEUER PROGRAMMVERSION SUCHEN

Vor der Installation wird geprüft, ob neuere Versionen von Kaspersky PURE auf den Updateservern von Kaspersky Lab vorhanden sind.

Wenn keine neuere Version des Programms auf den Updateservern von Kaspersky Lab gefunden wurde, wird der Installationsassistent für diese Version gestartet.

Wenn auf den Updateservern eine neuere Version von Kaspersky PURE vorgefunden wurde, werden Ihnen Download und Installation vorgeschlagen. Es wird empfohlen, die neue Programmversion zu installieren, da neue Versionen den Schutz Ihres Computers optimieren. Sollten Sie die Installation einer neueren Version ablehnen, wird der Installationsassistent für die laufende Version gestartet. Sollten Sie die Installation der neueren Version annehmen, werden die Programmdateien auf Ihren Computer kopiert und der Installationsassistent wird automatisch gestartet. Eine

weitere Beschreibung zur Installation einer neueren Version finden Sie in der Dokumentation zur entsprechenden Programmversion.

SCHRITT 2. SYSTEMKOMPATIBILITÄT FÜR INSTALLATION PRÜFEN

Bevor Kaspersky PURE auf Ihrem Computer installiert wird, wird die Kompatibilität des Betriebssystems und der Service Packs mit den Softwarevoraussetzungen für die Installation (s. S. 28) abgeglichen. Außerdem werden die Hardwarevoraussetzungen geprüft sowie die Rechte für die Installation des Programms. Wenn eine der aufgezählten Bedingung nicht erfüllt wird, erscheint eine entsprechende Meldung auf dem Bildschirm.

SCHRITT 3. INSTALLATIONSTYP AUSWÄHLEN

In dieser Phase der Installation können Sie den Typ für die Installation von Kaspersky PURE auswählen:

- *Schnelle Installation*. Bei dieser Variante (das Kontrollkästchen **Benutzerdefinierte Installation** ist deaktiviert) wird das Programm in vollem Umfang mit den von Kaspersky-Lab-Fachleuten empfohlenen Schutzeinstellungen auf Ihrem Computer installiert. Der Installationsassistent bietet Ihnen an, die Lizenzvereinbarung und die Erklärung zur Verwendung von Kaspersky Security Network zu lesen. Anschließend wird das Programm auf Ihrem Computer installiert.

- *Benutzerdefinierte Installation*. Bei Auswahl dieser Variante (das Kontrollkästchen **Benutzerdefinierte Installation** ist aktiviert) können Sie die Installationseinstellungen ändern: Sie können auswählen, welche Programmkomponenten installiert werden sollen und in welchen Ordner das Programm installiert wird. Für jede ausgewählte Komponente werden die von Kaspersky Lab empfohlenen Schutzeinstellungen verwendet.

  Die benutzerdefinierte Installationsmethode wird nur erfahrenen Anwendern empfohlen.

Unabhängig von der ausgewählten Variante können Sie beim Abschluss der Installation das Programm Kaspersky PURE aktivieren und den Programmschutz vor unbefugtem Zugriff anpassen.

Zum Fortsetzen der Installation klicken Sie auf **Weiter**.

SCHRITT 4. LIZENZVEREINBARUNG ANZEIGEN

In dieser Phase müssen Sie die Lizenzvereinbarung lesen, die zwischen Ihnen und Kaspersky Lab eingegangen wird.

Lesen Sie sich die Vereinbarung sorgfältig durch und wenn Sie mit allen Punkt einverstanden sind, klicken Sie auf **Akzeptieren**. Die Installation des Programms auf Ihrem Computer wird fortgesetzt.

Um die Programminstallation zu verwerfen, klicken Sie auf **Abbrechen**.

SCHRITT 5. ERKLÄRUNG ZUR VERWENDUNG VON KASPERSKY SECURITY NETWORK

Bei diesem Schritt wird Ihnen angeboten, an dem Programm Kaspersky Security Network teilzunehmen. Eine Beteiligung an diesem Programm sieht vor, dass Informationen über auf Ihrem Computer erkannte neue Bedrohungen, über gestartete Programme und über geladene signierte Programme an Kaspersky Lab geschickt werden. Außerdem werden ein einmaliger Identifikator, den Kaspersky PURE Ihrem Exemplar zuweist, sowie Systeminformationen gesendet. Es wird dabei garantiert, dass keine persönlichen Daten gesendet werden.

Lesen Sie sich die Erklärung zur Verwendung von Kaspersky Security Network gründlich durch. Um den gesamten Text der Vereinbarung aufzurufen, klicken Sie bitte auf die Schaltfläche **Vollständige KSN-Vereinbarung**. Wenn Sie mit allen Punkten einverstanden sind, setzen Sie das Häkchen im Kontrollkästchen **Ich akzeptiere die Teilnahmebedingungen für Kaspersky Security Network**.

Um die Installation fortzusetzen, klicken Sie auf **Installieren** (bei Express-Installation) oder auf **Weiter** (bei benutzerdefinierter Installation).

SCHRITT 6. ZIELORDNER AUSWÄHLEN

Dieser Schritt des Installationsassistenten ist verfügbar, wenn eine benutzerdefinierte Installation von Kaspersky PURE (s. S. 32) durchgeführt wird. Bei der standardmäßigen Installation wird dieser Schritt übersprungen und das Programm wird in dem standardmäßig hierfür vorgesehenen Ordner installiert.

Bei diesem Schritt können Sie den Ordner auswählen, in den Kaspersky PURE installiert werden soll. Standardmäßig gilt folgender Pfad:

- **<Datenträger> \ Program Files \ Kaspersky Lab \ Kaspersky PURE** – für 32-Bit-Systeme.
- **<Datenträger> \ Program Files (x86) \ Kaspersky Lab \ Kaspersky PURE** – für 64-Bit-Systeme.

Um Kaspersky PURE in einem anderen Ordner zu installieren, geben Sie den entsprechenden Pfad im Eingabefeld an oder klicken Sie auf **Durchsuchen** und wählen Sie im folgenden Fenster den gewünschten Ordner aus.

Bitte beachten Sie die folgenden Einschränkungen:

- Das Programm darf weder auf Netzlaufwerken oder Wechseldatenträgern noch auf virtuelle Laufwerken, die mit dem Befehl `SUBST` erstellt wurden, installiert werden.
- Es wird davor gewarnt, das Programm in einem Ordner zu installieren, der bereits Dateien oder andere Ordner enthält, da der Zugriff auf den Ordner anschließend verboten werden kann.
- Der Pfad des Installationsordners darf höchstens 160 Zeichen lang sein und keines der Sonderzeichen **/**, **?**, **:**, *****, **"**, **>**, **<** und **|** enthalten.

Zum Fortsetzen der Installation klicken Sie auf **Weiter**.

SCHRITT 7. PROGRAMMKOMPONENTEN FÜR INSTALLATION AUSWÄHLEN

Dieser Schritt des Installationsassistenten ist verfügbar, wenn eine benutzerdefinierte Installation von Kaspersky PURE (s. S. 32) durchgeführt wird. Bei der standardmäßigen Installation wird dieser Schritt übersprungen und das Programm wird vollständig auf dem Computer installiert.

Bei diesem Schritt können Sie die Programmkomponenten auswählen, die auf Ihrem Computer installiert werden soll. Standardmäßig sind alle Programmkomponenten und der Programmkern zur Installation vorgesehen.

Bei der Entscheidung über die Installation der einzelnen Komponenten bieten die Informationen im unteren Fensterbereich Hilfe. Sie beschreiben die Funktion einer Komponente und nennen den für die Installation benötigten Platz auf der Festplatte.

Um eine Komponente zur Installation auszuwählen, klicken Sie auf das Symbol neben dem Namen der Komponente und gehen Sie auf den Punkt **Komponente auf lokaler Festplatte installieren**. Damit eine Komponente nicht installiert wird, wählen Sie den Menüpunkt **Die Komponente wird nicht verfügbar sein** aus. Beachten Sie, dass die Abwahl der Installation von Anti-Virus-Komponenten dazu führt, dass kein Schutz vor einer ganzen Reihe von gefährlichen Programmen besteht.

Genaue Angaben über den freien Platz auf den Festplatten Ihres Computers erhalten Sie durch Klick auf **Laufwerk**. Die Informationen werden im folgenden Fenster angezeigt.

Klicken Sie auf **Weiter**, nachdem Sie die zur Installation gewünschten Komponenten gewählt haben. Um zur Liste mit den standardmäßig zu installierenden Komponenten zurückzugehen, klicken Sie auf **Zurück**.

SCHRITT 8. NACH ANDEREN ANTIVIREN-ANWENDUNGEN SUCHEN

Auf dieser Etappe erfolgt die Suche nach anderen auf Ihrem Computer installierten Antiviren-Produkten (einschließlich Kaspersky-Lab-Produkten), deren gleichzeitige Verwendung mit Kaspersky PURE zu Konflikten führen kann.

Beim Erkennen von solchen Programmen auf Ihrem Computer wird die Liste auf dem Bildschirm angezeigt. Ihnen wird deren Deinstallation vorgeschlagen, bevor Sie mit der Installation fortsetzen.

Verwenden Sie die Schaltfläche **Löschen**, um gefundene Antiviren-Programme zu entfernen.

Zum Fortsetzen der Installation klicken Sie auf **Weiter**.

SCHRITT 9. FIREWALL VON MICROSOFT WINDOWS DEAKTIVIEREN

Der Assistent führt diesen Schritt nur dann aus, wenn Kaspersky PURE auf einem Computer installiert wird, auf dem die Firewall von Microsoft Windows aktiviert ist, und wenn die Komponente Firewall zur Installation ausgewählt wurde.

Bei diesem Schritt der Installation von Kaspersky PURE wird Ihnen angeboten, die Firewall des Betriebssystems Microsoft Windows zu deaktivieren. Die zu Kaspersky PURE gehörende Komponente Firewall gewährleistet einen umfassenden Schutz bei der Arbeit in einem Netzwerk. Dadurch erübrigen sich zusätzliche Schutzwerkzeuge des Betriebssystems.

Wenn Sie die Komponente Firewall als primäres Schutzwerkzeug bei der Arbeit in einem Netzwerk verwenden möchten, klicken Sie auf **Weiter**. Die Firewall von Microsoft Windows wird in diesem Fall automatisch deaktiviert.

Wenn Sie Ihren Computer mit Hilfe der Firewall von Microsoft Windows schützen möchten, wählen Sie die Variante **Firewall von Microsoft Windows verwenden**. Die Komponente Firewall von Kaspersky PURE wird in diesem Fall zwar installiert. Um bei der Arbeit von Programmen Konflikte zu vermeiden, wird sie aber deaktiviert.

SCHRITT 10. INSTALLATION VORBEREITEN

Dieser Schritt des Installationsassistenten ist verfügbar, wenn eine benutzerdefinierte Installation von Kaspersky PURE (s. S. 32) durchgeführt wird. Bei der standardmäßigen Installation wird der Schritt übersprungen.

In dieser Phase wird Ihnen vorgeschlagen, die Vorbereitungen für die Installation von Kaspersky PURE auf Ihrem Computer abzuschließen.

Es wird davor gewarnt, bei der erstmaligen Installation des Programms das Kontrollkästchen **Installationsprozess schützen** zu deaktivieren. Wenn während der Programminstallation ein Fehler auftritt, kann der eingeschaltete Schutz für ein korrektes Rollback der Installation sorgen. Bei einer wiederholten Installation kann das Häkchen im Kontrollkästchen entfernt werden.

Bei einer Remote-Installation des Programms auf dem Computer über *Windows Remote Desktop* wird empfohlen, das Häkchen im Kontrollkästchen **Installationsprozess schützen** zu entfernen. Wenn das Häkchen im Kontrollkästchen stehen sollte, kann der Installationsvorgang nicht oder nicht richtig ausgeführt werden.

Zum Fortsetzen der Installation klicken Sie auf **Installieren**.

Im Verlauf der Installation unterbrechen die Komponenten von Kaspersky PURE, die den Datenverkehr im Netzwerk abfangen, die vorhandenen Netzwerkverbindungen. Die Mehrzahl der getrennten Verbindungen wird nach einiger Zeit wiederhergestellt.

SCHRITT 11. INSTALLATION

Die Installation des Programms nimmt einige Zeit in Anspruch. Warten Sie die Fertigstellung ab.

Nach der Installation wird automatisch der Konfigurationsassistent für Kaspersky PURE gestartet.

Falls bei der Installation ein Fehler auftritt, der möglicherweise durch auf dem Computer vorhandene schädliche Software verursacht wurde, die eine Installation von Antiviren-Programmen verhindern, schlägt der Installationsassistent vor, die spezielle Uitility *Kaspersky Virus Removal Tool* herunterzuladen, um die Infektion zu beseitigen.

Wenn Sie der Installation des Tools zustimmen, lädt der Installationsassistent es von den Kaspersky-Lab-Servern herunter und startet anschließend automatisch die Installation des Tools. Gelingt dem Assistenten der Download des Tools nicht, so werden Sie aufgefordert, es über einen Link manuell herunterzuladen.

Nachdem das Tool seine Arbeit abgeschlossen hat, muss es entfernt werden. Anschließend wird die Installation von Kaspersky PURE erneut gestartet.

SCHRITT 12. PROGRAMM AKTIVIEREN

Durch die *Aktivierung* erlangt die Lizenz für die Nutzung der Vollversion des Programms ihre Gültigkeit für den entsprechenden Zeitraum.

Um das Programm zu aktivieren, ist eine Internetverbindung erforderlich.

Für die Aktivierung von Kaspersky PURE bestehen folgende Möglichkeiten:

- **Kommerzielle Version aktivieren**. Wählen Sie diese Option aus und geben Sie den Aktivierungscode (s. Abschnitt "О коде активации" auf S. 43), wenn Sie die kommerzielle Programmversion erworben haben.

- **Testversion aktivieren**. Wählen Sie diese Aktivierungsvariante, wenn Sie eine Testversion des Programms installieren möchten, bevor Sie über den Kauf einer kommerziellen Version entscheiden. Für die Gültigkeitsdauer der Lizenz für die Testversion können Sie das Programm mit uneingeschränktem Funktionsumfang verwenden. Nach Ablauf der Lizenz ist es nicht möglich, erneut eine Testlizenz zu aktivieren.

- **Später aktivieren**. Bei der Auswahl dieser Variante wird die Aktivierung von Kaspersky PURE übersprungen. Das Programm wird auf Ihrem Computer installiert, wobei bestimmte Programmfunktionen nicht genutzt werden können. Dazu gehören z.B. Update (nach der Installation ist die Aktualisierung nur ein Mal möglich), Anlegen eines verschlüsselten Containers und Zusätzliche Funktionen. Die Variante **Später aktivieren** steht nur zur Verfügung, wenn der Aktivierungsassistent zum ersten Mal gleich nach der Programminstallation gestartet wird.

SCHRITT 13. DATEN ÜBERPRÜFEN

Bei diesem Schritt sendet Kaspersky PURE Daten zur Überprüfung an den Aktivierungsserver.

Zur Überprüfung der Daten ist eine Internetverbindung erforderlich.

SCHRITT 14. ANMELDUNG DES BENUTZERS

Dieser Schritt ist nur bei der Aktivierung einer kommerziellen Programmversion verfügbar. Bei der Aktivierung einer Testversion wird der Schritt übersprungen.

Um auch weiterhin die Möglichkeit zu haben, den Technischen Support von Kaspersky Lab zu kontaktieren, müssen Sie sich registrieren.

Wenn Sie mit der Anmeldung einverstanden sind, füllen Sie die entsprechenden Felder aus und klicken Sie dann auf **Weiter**, um Ihre Anmeldung abzuschicken.

SCHRITT 15. AKTIVIERUNG ABSCHLIEßEN

Der Konfigurationssassistent informiert Sie darüber, dass die Aktivierung von Kaspersky PURE erfolgreich abgeschlossen wurde. Außerdem werden Informationen über die Lizenz angezeigt: Typ (kommerziell oder Test), Gültigkeitsdauer der Lizenz, sowie Anzahl der Computer, für die die Lizenz gültig ist.

Bei der Aktivierung eines Abonnements werden anstelle des Ablaufdatums für die Lizenz Informationen zum Abo-Status (s. S. 256) angezeigt.

Klicken Sie auf den Link **Weiter**, um den Assistenten fortzusetzen.

SCHRITT 16. KONTROLLE DES ZUGRIFFS AUF DAS PROGRAMM

Dieser Schritt des Installationsassistenten ist verfügbar, wenn eine benutzerdefinierte Installation von Kaspersky PURE (s. S. 32) durchgeführt wird. Bei der standardmäßigen Installation wird dieser Schritt übersprungen und das Programm wird ohne Zugriffsbeschränkungen installiert. Sie können diese Beschränkungen später manuell im Programmkonfigurationsfenster aktivieren (s. S. 77).

Die Zugriffskontrolle für Kaspersky PURE erlaubt es, das unerlaubte Ausschalten des Schutzes und das Ändern von Einstellungen der Komponenten von Kaspersky PURE zu verhindern.

Die Einschränkung des Zugriffs mit Hilfe eines Kennworts kann in folgenden Fällen von Nutzen sein:

- Wenn ein PC von mehreren Personen verwendet wird, die über unterschiedliche Fertigkeiten im Umgang mit Computern verfügen.
- Wenn Kaspersky PURE für die Sicherheit mehrerer Computer verantwortlich ist, die zu einem lokalen Netzwerk gehören.
- Wenn ein Risiko besteht, dass der Schutz durch Schadprogramme ausgeschaltet werden kann.

Um den Kennwortschutz zu verwenden, aktivieren Sie das Kontrollkästchen **Kennwortschutz aktivieren** und füllen Sie die Felder **Kennwort** und **Kennwort bestätigen** aus.

Geben Sie darunter den Bereich an, auf den sich die Zugriffsbeschränkung beziehen soll:

- **Programmparameter ändern** – Kennwortabfrage beim Versuch des Benutzers, geänderte Einstellungen von Kaspersky PURE zu speichern.
- **Backup für Daten verwalten** – Kennwortabfrage vor dem Start einer Backup-Aufgabe.
- **Kindersicherung verwalten** – Kennwortabfrage vor dem Start der Aufgabe Kindersicherung.
- **Ferngesteuerte Sicherheitsverwaltung auf den Computern des Heimnetzwerks** – Kennwortabfrage, bevor die Einstellungen von Kaspersky PURE im Remote-Modus geändert werden.
- **Programm beenden** – Kennwortabfrage beim Versuch des Benutzers, die Arbeit des Programms zu beenden.

SCHRITT 17. SCHUTZMODUS AUSWÄHLEN

Dieser Schritt des Installationsassistenten ist verfügbar, wenn eine benutzerdefinierte Installation von Kaspersky PURE (s. S. 32) durchgeführt wird. Bei der standardmäßigen Installation wird dieser Schritt übersprungen und das Programm arbeitet im automatischen Schutzmodus. Sie können später manuell einen Schutzmodus auswählen (s. S. 61).

Wählen Sie einen Modus für den Schutz, der von Kaspersky PURE gewährleistet wird.

Es stehen zwei Modi zur Auswahl:

- *Automatisch*. Beim Eintreten wichtiger Ereignisse führt Kaspersky PURE automatisch die von Kaspersky Lab empfohlene Aktion aus. Beim Fund einer Bedrohung versucht das Programm, das Objekt zu desinfizieren, und wenn die Desinfektion fehlschlägt, wird das Objekt gelöscht. Verdächtige Objekte werden unbearbeitet übersprungen. Über eingetretene Ereignisse wird durch Popupmeldungen informiert.

- *Interaktiv*. In diesem Modus reagiert das Programm so auf eintretende Ereignisse, wie Sie es festlegen. Beim Eintreten von Ereignissen, die Ihre Reaktion erfordern, zeigt das Programm auf dem Bildschirm eine Meldung an, in der eine Aktion gewählt werden kann.

Meldunge über den Fund einer aktiven Infektion werden unabhängig vom ausgewählten Schutzmodus auf dem Bildschirm angezeigt.

SCHRITT 18. PROGRAMM-UPDATE ANPASSEN

Dieser Schritt des Installationsassistenten ist verfügbar, wenn eine benutzerdefinierte Installation von Kaspersky PURE (s. S. 32) durchgeführt wird. Bei der standardmäßigen Installation wird dieser Schritt übersprungen und es wird standardmäßig das automatische Update ausgeführt. Sie können später manuell einen Updatemodus auswählen (s. S. 97).

Die Qualität des Schutzes Ihres Computers ist unmittelbar vom rechtzeitigen Download der Updates für die Datenbanken und Programm-Module abhängig. In diesem Fenster des Assistenten können Sie den Modus für das Update auswählen und Einstellungen für den Zeitplan vornehmen:

- **Automatisches Update**. Das Programm prüft in festgelegten Zeitabständen, ob an der Updatequelle ein Updatepaket vorhanden ist. Die Häufigkeit der Überprüfung kann während Viren-Epidemien steigen und unter gewöhnlichen Umständen sinken. Wenn neue Updates gefunden werden, lädt das Programm sie herunter und installiert sie auf dem Computer. Dieser Modus wird standardmäßig verwendet.

- **Update nach Zeitplan** (Das Intervall ist von den Zeitplaneinstellungen abhängig). Das Update wird automatisch nach einem festgelegten Zeitplan gestartet. Der Zeitplan wird in dem Fenster angepasst, das durch Klick auf **Einstellungen** geöffnet wird.

- **Manuelles Update**. In diesem Fall starten Sie das Programm-Update manuell.

Beachten Sie, dass die Datenbanken und Programm-Module, die in der Distribution enthalten sind, zum Zeitpunkt der Installation von Kaspersky PURE bereits veraltet sein können. Wir empfehlen deshalb, die aktuellen Updates herunterzuladen. Klicken Sie dazu auf **Jetzt aktualisieren**. In diesem Fall empfängt das Programm die erforderlichen Updates von den Updateseiten im Internet und installiert sie auf Ihrem Computer.

Wenn die im Lieferumfang enthaltenen Datenbanken stark veraltet sind, kann das Updatepaket relativ umfangreich sein und zusätzlichen Internet-Datenverkehr verursachen (bis zu mehrere Dutzend MB).

Klicken Sie auf **Einstellungen**, um die Update-Einstellungen anzupassen (die Ressource auswählen, von der das Update erfolgt; den Start des Updates mit den Rechten eines bestimmten Benutzerkontos anpassen usw.).

SCHRITT 19. ERKENNBARE BEDROHUNGEN AUSWÄHLEN

Dieser Schritt des Installationsassistenten ist verfügbar, wenn eine benutzerdefinierte Installation von Kaspersky PURE (s. S. 32) durchgeführt wird. Bei der standardmäßigen Installation wird dieser Schritt übersprungen und die Standardeinstellungen werden festgelegt. Sie können später manuell die erkennbaren Bedrohungen auswählen (s. S. 227).

Auf dieser Etappe können Sie die Kategorien der Bedrohungen auswählen, vor denen Kaspersky PURE Ihren Computer schützen soll. Programme, die Ihrem Computer Schaden zufügen können, werden immer von Kaspersky PURE gesucht. Dazu gehören die Programmtypen Viren, Würmer und trojanische Programme.

SCHRITT 20. SYSTEMANALYSE

Auf dieser Etappe werden Informationen über Programme, die zu Microsoft Windows gehören, gesammelt. Diese Programme werden in die Liste der vertrauenswürdigen Anwendungen aufgenommen, deren Aktionen im System nicht beschränkt werden.

Andere Programme werden nach der Installation von Kaspersky PURE analysiert, wenn sie zum ersten Mal gestartet werden.

SCHRITT 21. ASSISTENT ABSCHLIEßEN

Das letzte Fenster des Konfigurationsassistenten informiert über den Abschluss der Programminstallation. Um mit der Arbeit von Kaspersky PURE zu beginnen, vergewissern Sie sich, dass das Kontrollkästchen **Kaspersky PURE starten** aktiviert ist und klicken Sie auf **Beenden**.

In einigen Fällen kann ein Neustart des Betriebssystems erforderlich sein. Wenn Sie das Kontrollkästchen **Kaspersky PURE starten** vor dem Abschluss des Assistenten aktiviert haben, wird das Programm nach einem Neustart automatisch gestartet. Wenn Sie dieses Kontrollkästchen deaktiviert haben, muss das Programm manuell (s. S. 58) gestartet werden.

ERSTE SCHRITTE

Nach abgeschlossener Installation und Konfiguration ist das Programm einsatzbereit. Um einen effektiven Schutz Ihres Computers zu gewährleisten, empfehlen wir direkt im Anschluss an die Installation und Konfiguration die Durchführung folgender Aktionen:

- Programm-Datenbanken aktualisieren (s. Abschnitt "Aktualisierung von Programmdatenbanken und -modulen" auf S. 65).
- Computer auf Viren (s. Abschnitt "Wie eine vollständige Virenuntersuchung des Computers ausgeführt wird" auf S. 68) und Schwachstellen untersuchen.
- Schutzstatus des Computers prüfen (auf S.) und bei Bedarf Probleme im Schutz beheben (s. Abschnitt "Probleme im Computerschutz diagnostizieren und beheben" auf S. 59).

Die Komponente Anti-Spam, die zu Kaspersky PURE gehört, verwendet einen lernfähigen Algorithmus zum Erkennen unerwünschter E-Mails. Starten Sie den Trainingsassistenten für Anti-Spam, um die Komponente auf die Arbeit mit Ihren E-Mails einzustellen.

Passen Sie das Backup (s. Abschnitt "Wie Sicherungskopien Ihrer Daten angelegt werden" auf S. 76) an, um Daten bei Verlust schnell wiederherzustellen.

Legen Sie verschlüsselte Container für die Datenspeicherung an (s. Abschnitt "Datenverschlüsselung" auf S. 72), um sensible Daten vor unbefugtem Zugriff zu schützen

Passen Sie die Kindersicherung an (s. Abschnitt "Wie die Verwendung des Computers und Internets für verschiedene Benutzer eingeschränkt wird" auf S. 78), um Kinder und Jugendliche vor Gefahren zu schützen, die bei der Arbeit am Computer bestehen.

PROGRAMM MIT HILFE DES INSTALLATIONSASSISTENTEN ÄNDERN, REPARIEREN ODER LÖSCHEN

Die Reparatur des Programms kann dann von Nutzen sein, wenn Sie Fehler in seiner Arbeit feststellen, die auf fehlerhafte Einstellungen oder beschädigte Programmdateien zurückgehen.

Das Ändern des Komponentenbestands erlaubt Ihnen, bestimmte Komponenten von Kaspersky PURE nachträglich zu installieren oder jene Komponenten zu löschen, die bei der Arbeit stören oder überflüssig sind.

- *Gehen Sie folgendermaßen vor, um den ursprünglichen Programmzustand wiederherzustellen, um Komponenten von Kaspersky PURE, die bei der Erstinstallation nicht installiert wurden, zu installieren, oder um das Programm zu löschen:*

  1. Legen Sie die CD mit der Programmdistribution in das CD/DVD-ROM-Laufwerk ein, wenn die Installation von dort aus erfolgte. Wenn die Installation von Kaspersky PURE aus einer anderen Quelle erfolgte (z.B. gemeinsamer Ordner, Ordner auf der Festplatte), vergewissern Sie sich, dass die Programmdistribution in diesem Ordner vorhanden ist und Sie zugriffsberechtigt sind.

  2. Wählen Sie **Start** → **Programme** → **Kaspersky PURE9.1** → **Ändern, Reparieren oder Löschen**.

Dadurch wird das Installationsprogramm gestartet, das die Form eines Assistenten besitzt. Im Folgenden werden die Schritte zur Reparatur, zum Ändern des Bestands der Programmkomponenten und zum Löschen des Programms ausführlich beschrieben.

IN DIESEM ABSCHNITT

Schritt 1. Startfenster des Installationsprogramms 40

Schritt 2. Operation wählen 40

Schritt 3. Operation zum Reparieren, Ändern oder Löschen des Programms abschließen 41

SCHRITT 1. STARTFENSTER DES INSTALLATIONSPROGRAMMS

Wenn Sie alle oben beschriebenen Aktionen ausgeführt haben, die für die Reparatur oder das Ändern des Komponentenbestands erforderlich sind, wird auf dem Bildschirm das Begrüßungsfenster des Installationsprogramms für Kaspersky PURE geöffnet. Klicken Sie auf **Weiter**, um fortzufahren.

SCHRITT 2. OPERATION WÄHLEN

Auf dieser Etappe müssen Sie festlegen, welche Operation Sie mit dem Programm vornehmen möchten: Zur Auswahl stehen das Ändern des Komponentenbestands, das Wiederherstellen des ursprünglichen Zustands der installierten Komponenten oder das Löschen bestimmter Komponenten oder des ganzen Programms. Klicken Sie zum Ausführen einer Operation auf die entsprechende Schaltfläche. Die weiteren Aktionen des Installationsprogramms sind von der gewählten Operation abhängig.

Das Vorgehen beim Ändern des Komponentenbestands entspricht der benutzerdefinierten Installation des Programms: Sie können festlegen, welche Komponenten installiert und welche gelöscht werden sollen.

Die Reparatur des Programms erfolgt auf Basis der installierten Komponenten. Alle Dateien der installierten Komponenten werden aktualisiert und für jede dieser Komponenten wird die **empfohlene** Sicherheitsstufe eingestellt.

Beim Löschen des Programms können Sie wählen, welche Daten, die bei der Arbeit des Programms erstellt und verwendet wurden, auf Ihrem Computer gespeichert werden sollen. Um alle Daten von Kaspersky PURE zu löschen,

wählen Sie die Variante **Anwendung vollständig löschen**. Um bestimmte Daten zu speichern, wählen Sie die Variante **Objekte der Anwendung speichern** und geben Sie an, welche Objekte beibehalten werden sollen:

- *Aktivierungsdaten* – Schlüsseldatei, die für die Arbeit des Programms erforderlich ist.
- *Anti-Spam-Datenbank* – Datenbank, auf deren Basis unerwünschte E-Mails erkannt werden können. Diese Datenbank enthält detaillierte Informationen darüber, welche Mails für Sie als Spam gelten und welche als nützlich.
- *Quarantäne- und Backup-Objekte*. Backup-Objekte – Sicherungskopien von gelöschten oder desinfizierten Objekten. Es wird empfohlen, diese Objekte zu speichern, um sie bei Bedarf später wiederherzustellen. *Quarantäneobjekte* – Objekte, die möglicherweise von Viren oder Virusmodifikationen infiziert sind. Solche Objekte enthalten Code, der Ähnlichkeit mit dem Code eines bekannten Virus besitzt. Allerdings lässt sich nicht sicher sagen, ob sie schädlich sind. Es wird empfohlen, diese Objekte zu speichern. Möglicherweise erweisen sie sich nach einem Update der Programm-Datenbanken als virenfrei oder können desinfiziert werden.
- *Schutzparameter* – Parameterwerte für die Arbeit aller Programmkomponenten.
- *iSwift- und iChecker-Daten* – Datenbank, die Informationen über untersuchte Objekte des NTFS-Dateisystems enthält. Sie erlaubt die Beschleunigung der Objektuntersuchung. Bei Einsatz dieser Datenbank untersucht Kaspersky PURE nur jene Objekte, die seit der letzten Untersuchung verändert wurden.
- *Daten des gemeinsamen Ordners der Sicheren Umgebung* – Daten, die im SaveRun-Modus und in der gewöhnlichen Umgebung verfügbar sind.

Wenn zwischen der Deinstallation einer Version von Kaspersky PURE und der Installation einer anderen Version ein relativ großer Zeitraum liegt, wird davon abgeraten, die aus der vorherigen Programminstallation stammende iSwift- und iChecker-Datenbank zu verwenden. In der Zwischenzeit kann ein gefährliches Programm auf den Computer gelangt sein, dessen schädliche Aktionen bei Verwendung dieser Datenbank nicht erkannt werden, was zu einer Infektion des Computers führen kann.

Klicken Sie auf **Weiter**, um die gewählte Operation zu starten. Der Prozess zum Kopieren der notwendigen Dateien auf Ihren Computer oder zum Löschen der ausgewählten Komponenten und Daten wird gestartet.

SCHRITT 3. OPERATION ZUM REPARIEREN, ÄNDERN ODER LÖSCHEN DES PROGRAMMS ABSCHLIEßEN

Der Fortschritt des Prozesses zum Reparieren, Ändern oder Löschen wird auf dem Bildschirm dargestellt. Danach erfolgt ein Hinweis auf den Abschluss der Operation.

Die Deinstallation macht in der Regel einen Neustart des Computers erforderlich, um Änderungen im System zu berücksichtigen. Auf dem Bildschirm erscheint eine Anfrage für den Neustart des Computers. Klicken Sie auf **Ja**, um sofort einen Neustart vorzunehmen. Um den Computer später auf Befehl neu zu starten, klicken Sie auf **Nein**.

LIZENZVERWALTUNG

Dieser Abschnitt informiert über die wichtigsten Begriffe, die mit der Programmlizenzierung zusammenhängen. In diesem Abschnitt erfahren Sie außerdem, wie die Gültigkeitsdauer für eine Lizenz automatisch verlängert werden kann und wo sich Informationen zur aktiven Lizenz befinden.

IN DIESEM ABSCHNITT

Über den Lizenzvertrag 42

Über die Lizenz 42

Über den Aktivierungscode 43

Lizenz-Info anzeigen 43

ÜBER DEN LIZENZVERTRAG

Der *Lizenzvertrag* ist ein Vertrag zwischen einer natürlichen oder juristischen Person, die rechtmäßiger Besitzer eines Exemplars von Kaspersky PURE ist, und der Kaspersky Lab ZAO. Der Lizenzvertrag gehört zum Lieferumfang jedes Kaspersky-Lab-Programms. Er legt die Rechte und Einschränkungen für die Nutzung von Kaspersky PURE genau fest.

In Übereinstimmung mit dem Lizenzvertrag erhalten Sie durch den Erwerb und die Installation eines Kaspersky-Lab-Programms das unbefristete Besitzrecht an einer Kopie.

ÜBER DIE LIZENZ

Die *Lizenz* verleiht das Recht zur Nutzung von Kaspersky PURE und der zum Programm gehörenden Zusatzleistungen, die von Kaspersky Lab und seinen Partnern angeboten werden.

Jede Lizenz wird durch Gültigkeitsdauer und Typ charakterisiert.

Die *Gültigkeitsdauer einer Lizenz* ist die Zeitspanne, für die Ihnen die Zusatzleistungen zur Verfügung stehen.

- Technischer Support.
- Update der Datenbanken und Module des Programms.

Der Umfang der angebotenen Leistungen ist vom Lizenztyp abhängig.

Es sind folgende Lizenztypen vorgesehen

- *Test* – Kostenlose Lizenz mit begrenzter Gültigkeitsdauer (z.B. 30 Tage) zum Kennenlernen von Kaspersky PURE.

  Eine Testlizenz kann nur einmal verwendet werden.

  Eine Testlizenz wird zusammen mit einer Testversion des Programms geliefert. Wenn Sie eine Testlizenz verwenden, ist der Technische Support auf Fragen über die Programmaktivierung und den Kauf einer kommerziellen Lizenz beschränkt. Nach Ablauf der Gültigkeitsdauer einer Testlizenz stellt Kaspersky PURE alle Funktionen ein. Um mit dem Programm weiterzuarbeiten, ist eine Aktivierung notwendig.

- *Kommerziell* – Gekaufte Lizenz, die eine begrenzte Gültigkeitsdauer (z.B. 1 Jahr) besitzt und beim Kauf von Kaspersky PURE zur Verfügung gestellt wird. Für jede Lizenz ist eine bestimmte Anzahl von Computern festgelegt, auf die Kaspersky PURE mit dieser Lizenz installiert werden darf.

  Während der Laufzeit einer kommerziellen Lizenz sind alle Programmfunktionen und zusätzliche Services verfügbar.

  Nach Ablauf der Gültigkeitsdauer einer kommerziellen Lizenz führt Kaspersky PURE seine Funktionen weiterhin aus, allerdings werden die Antiviren-Datenbanken nicht mehr aktualisiert. Sie können Ihren Computer weiterhin auf Viren untersuchen und die Schutzkomponenten verwenden, jedoch nur mit den Antiviren-Datenbanken , die bei Ablauf der Lizenz aktuell waren. Sie werden zwei Wochen vor Ablauf der Lizenz vom Programm benachrichtigt und können rechtzeitig die Gültgkeitsdauer der Lizenz verlängern.

- *Kommerzielle Lizenz mit Update-Abonnement* und *kommerzielle Update- und Schutz-Lizenz* – Gekaufte Lizenz mit flexiblen Einsatzmöglichkeiten: Sie können das Abonnement anhalten und fortsetzen, die Gültigkeitsdauer des Abos im automatischen Modus verlängern oder das Abo kündigen. Eine Lizenz mit Abonnement wird von Dienstleistern angeboten. Das Abonnement wird über den persönlichen Bereich des Benutzers auf der Webseite des Dienstleisters verwaltet.

  Ein Abonnement kann eine begrenzte Laufzeit besitzen (z.B. für 1 Jahr) oder unbegrenzt sein. Ein Abonnement mit begrenzter Laufzeit muss bei Ablauf der Gültigkeitsdauer vom Benutzer verlängert werden. Ein Abonnement mit unbegrenzter Laufzeit wird automatisch verlängert, falls der erforderliche Betrag rechtzeitig an den Dienstleister überwiesen wird.

  Wenn die Abonnementlaufzeit begrenzt ist, wird Ihnen eine Ermässigungsfrist zur Verlängerung des Abos eingeräumt, während der die Funktionsfähigkeit des Programms erhalten bleibt.

  Wenn ein Abonnement nicht verlängert wird, lädt Kaspersky PURE nach Ablauf der Ermäßigungsfrist keine Updates für die Programm-Datenbanken mehr herunter (für eine Lizenz mit Update-Abonnement), stellt den Computerschutz ein und startet keine Untersuchungsaufgaben (für eine Lizenz mit Update- und Schutz-Abonnement).

  Bei Verwendung eines Abonnements können Sie keinen anderen Aktivierungscode verwenden, um die Gültigkeit einer Lizenz zu verlängern. Das ist erst nach Ablauf des Abonnements möglich.

  Wenn im Augenblick der Abonnementsaktivierung eine Lizenz mit beschränkter Gültigkeitsdauer aktiviert wurde, wird diese durch eine neue Lizenz mit Abonnement ersetzt. Um ein Abonnement zu kündigen, wenden Sie sich an den Dienstleister, bei dem Sie Kaspersky PURE erworben haben.

  Abhängig vom Händler können die Aktionen mit dem Abonnement unterschiedlich sein. Außerdem kann es sein, dass Ihnen keine Ermässigungsfrist gewährt wird, während der das Abo verlängert werden kann.

ÜBER DEN AKTIVIERUNGSCODE

Ein *Aktivierungscode* ist ein Code, den Sie beim Kauf einer kommerziellen Lizenz für Kaspersky PURE erhalten. Dieser Code ist für die Programmaktivierung erforderlich.

Der Aktivierungscode besteht aus einer durch Bindestriche getrennten Folge von lateinischen Buchstaben und Ziffern, die in vier Blöcken zu je fünf Zeichen angeordnet sind (Beispiel: AA111-AA111-AA111-AA111).

LIZENZ-INFO ANZEIGEN

➧ *Gehen Sie folgendermaßen vor, um Informationen zur aktiven Lizenz anzuzeigen:*

1. Öffnen Sie das Programmhauptfenster.
2. Öffnen Sie mit dem Link **Lizenz** im unteren Fensterbereich das Fenster **Lizenzverwaltung**.

In diesem Fenster können Sie den Vorgang zur Programmaktivierung starten, eine neue Lizenz erwerben oder die Gültigkeitsdauer für die aktive Lizenz verlängern.

Abbildung 1. Fenster Lizenzen verwalten

PROGRAMMOBERFLÄCHE

In diesem Kapitel werden die wichtigsten Elemente der Oberfläche von Kaspersky PURE beschrieben.

IN DIESEM ABSCHNITT

Symbol im Infobereich der Taskleiste 45

Kontextmenü 46

Hauptfenster von Kaspersky PURE 47

Programmkonfigurationsfenster 55

Meldungsfenster und Popupmeldungen 56

SYMBOL IM INFOBEREICH DER TASKLEISTE

Sofort nach der Installation von Kaspersky PURE erscheint sein Symbol im Infobereich der Taskleiste von Microsoft Windows.

Das Symbol besitzt folgende Funktionen:

- Es dient als Indikator für die Arbeit des Programms.
- Es bietet Zugriff auf das Kontextmenü, das Programmhauptfenster und das Nachrichtenfenster.

Indikator für die Programmarbeit

Das Symbol dient als Indikator für die Arbeit des Programms. Es informiert über den Schutzstatus und zeigt eine Reihe wichtiger Aktionen, die vom Programm ausgeführt werden.

– Es wird eine E-Mail-Nachricht untersucht.

– Der Web-Datenverkehr wird untersucht.

– Die Datenbanken und die Programm-Module werden aktualisiert.

– Der Neustart des Computers ist erforderlich, um die Updates zu übernehmen.

– Bei der Arbeit einer Programmkomponente ist eine Störung aufgetreten.

Die Animation des Symbols ist standardmäßig aktiviert: Beispielsweise erscheint bei der Untersuchung einer E-Mail im Hintergrund des Programmsymbols das Piktogramm eines Briefs, beim Update der Programm-Datenbanken erscheint ein rotierender Globus. Sie können die Animation ausschalten (s. S. 231).

Wenn die Animation aktiviert ist, kann das Symbol folgendes Aussehen annehmen:

(farbiges Symbol) – Alle oder einige Schutzkomponenten sind aktiv.

(schwarzweißes Symbol) – Alle Schutzkomponenten wurden deaktiviert.

Zugriff auf das Kontextmenü und auf die Programmfenster

Mit Hilfe des Symbols können Sie das Kontextmenü (s. S. 46) und das Programmhauptfenster (s. S. 47) öffnen.

- *Um das Kontextmenü zu öffnen,*

  zeigen Sie mit der Maus auf das Symbol und führen Sie einen Rechtsklick aus.

- *Um das Programmhauptfenster zu öffnen:*

  zeigen Sie mit der Maus auf das Symbol und führen Sie einen Linksklick aus.

Wenn Nachrichten von Kaspersky Lab erschienen sind, wird im Infobereich der Taskleiste von Microsoft Windows das Symbol eingeblendet. Das Fenster mit Neuigkeiten (s. S. 231) kann durch Doppelklick auf dieses Symbol geöffnet werden.

KONTEXTMENÜ

Das Kontextmenü bietet Zugriff auf die wichtigsten Schutzaufgaben.

Das Menü von Kaspersky PURE enthält folgende Punkte:

- **Update** – startet die Aktualisierung der Programmdatenbanken und -module.
- **Computer vollständig untersuchen** – startet eine vollständige Untersuchung des Computers auf das Vorhandensein schädlicher Objekte (s. S. 68).
- **Auf Viren untersuchen** – startet die Untersuchung der ausgewählten Objekte auf das Vorhandensein schädlicher Objekte (s. S. 66).
- **Virtuelle Tastatur** – öffnet die virtuelle Tastatur (s. S. 71).
- **Kaspersky PURE** – öffnet das Programmhauptfenster (s. S. 47).
- **Einstellungen** – öffnet das Fenster zur Konfiguration der Funktionsparameter des Programms (s. S. 55).
- **Aktivierung** – startet den Aktivierungsassistenten für Kaspersky PURE. Dieser Menüpunkt ist nur vorhanden, wenn das Programm noch nicht aktiviert wurde.
- **Über das Programm** – Infofenster mit Angaben zum Programm öffnen.
- **Schutz anhalten / fortsetzen** – Arbeit der Echtzeitschutz-Komponenten vorübergehend deaktivieren / wieder aktivieren. Dieser Menüpunkt bezieht sich nicht auf das Programm-Update und die Ausführung von Aufgaben zur Virensuche.
- **Kindersicherung anhalten / aktivieren** – Kontrolle für alle Benutzer vorübergehend deaktivieren / aktivieren. Dieser Menüpunkt ist nur vorhanden, wenn die Komponente Kindersicherung installiert wurde.
- **Netzwerkverkehr blockieren / Netzwerkverkehr freigeben** – vorübergehende Sperrung / Freigabe aller Netzwerkverbindungen des Computers.

- **Beenden** – Arbeit von Kaspersky PURE beenden (bei Auswahl dieses Menüpunkts wird das Programm aus dem Arbeitsspeicher des Computers entfernt).

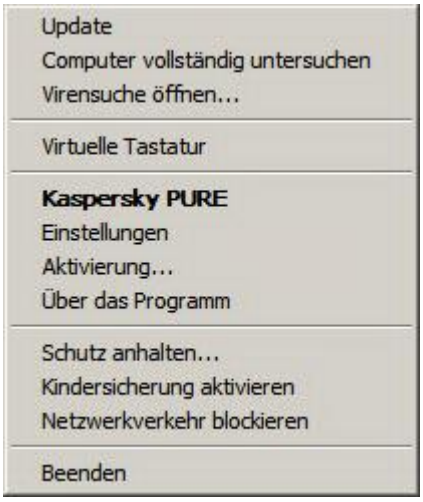


Abbildung 2. Kontextmenü

Wird das Kontextmenü geöffnet, während eine Untersuchungsaufgabe oder Updateaufgabe läuft, so wird ihr Name mit Prozentangabe für das Ausführungsergebnis im Kontextmenü angezeigt. Durch die Auswahl des Menüpunkts mit dem Aufgabennamen gelangen Sie in das Hauptfenster mit einem Bericht über die aktuellen Ausführungsergebnisse.

Um das Kontextmenü zu öffnen,

zeigen Sie im Infobereich der Taskleiste mit der Maus auf das Programmsymbol und führen Sie einen Rechtsklick aus.

HAUPTFENSTER VON KASPERSKY PURE

Die Elemente des Hauptfensters bieten Zugriff auf die Hauptfunktionen des Programms.

Das Hauptfenster lässt sich bedingt in drei Bereiche aufteilen:

- Der obere Bereich des Fensters informiert über den aktuellen Schutzstatus Ihres Computers.

Es gibt drei Varianten für den Schutzstatus. Jeder Status wird durch eine bestimmte Farbe signalisiert. Die Farbe Grün bedeutet, dass der Schutz Ihres Computers dem erforderlichen Niveau entspricht. Gelb und Rot warnen vor unterschiedlichen Sicherheitsrisiken. Als Bedrohung gilt nicht nur der Fund schädlicher Programme, sondern auch die Verwendung veralteter Datenbanken, die deaktivierten Schutzkomponenten, die Auswahl einer niedrigen Sicherheitsstufe u.a.

Vorhandene Sicherheitsrisiken sollten umgehend behoben (s. Abschnitt "Probleme im Schutz diagnostizieren und beheben" auf S. 59) werden.

- Der mittlere Fensterbereich bietet Zugriff auf die Hauptfunktionen des Programms. Außerdem sind hier folgende Aktionen möglich: Schutz fortsetzen / anhalten, Virensuche ausführen, Datensicherung starten u.a. Im oberen Fensterbereich befinden sich folgende Hauptkomponenten von Kaspersky PURE:

  - **Backup** – Sicherungskopien von Dateien anlegen und speichern. Aus Sicherungskopien lassen sich bei Verlust Daten wiederherstellen.

- **Computersicherheit** – Komponenten, die den Computer vor verschiedenen Bedrohungen schützen.
- **Kindersicherung** – kontrolliert den Zugriff von Benutzern auf den Computer und auf Internetressourcen.

- Der untere Fensterbereich erlaubt den Zugriff auf Zusatzfunktionen, die einem erweiterten Schutz dienen und die Arbeit des Systems optimieren können. Im unteren Fensterbereich befinden sich folgende Komponenten und Dienste:
  - **Zusätzliche Funktionen** – Systemeinstellungen optimieren und spezifische Aufgaben, die der Computersicherheit dienen, ausführen.
  - **Virtuelle Tastatur** – Ausspähen von über die Tastatur eingegebenen Daten vorbeugen.
  - **Verwaltung –** Remote-Administration von Kaspersky PURE (s. S. 191) **.**
  - **Datenverschlüsselung** – unbefugten Zugriff auf vertrauliche Daten verhindern.
  - **Password Manager** – Schutz persönlicher Daten wie Kennwörter, Benutzernamen, ICQ-Nummern, Kontaktdaten usw.

Abbildung 3. Programmhauptfenster

Außerdem stehen folgende Schaltflächen und Links zur Verfügung:

- **Einstellungen** – wechselt zu den allgemeinen Programmeinstellungen (s. S. 55).
- **Hilfe** – Hilfesystem für Kaspersky PURE öffnen.
- **Mein Kaspersky Account** – in den persönlichen Bereich des Benutzers (https://my.kaspersky.de) auf der Seite des Technischen Supports gehen.

- **Support** - Das Fenster mit Informationen über das System und mit Links zu Informationsressourcen von Kaspersky Lab (Webseite des Technischen Supports, Forum) öffnen.

- **Lizenz** – zur Aktivierung von Kaspersky PURE bzw. zur Lizenzverlängerung wechseln.

Sie können das Aussehen von Kaspersky PURE verändern (s. Abschnitt "Aussehen des Programms" auf S 230), indem Sie grafische Elemente und Farbschemen erstellen und verwenden..

COMPUTERSICHERHEIT

Das Fenster **Computersicherheit** lässt sich bedingt in zwei Bereiche aufteilen:

- Die linke Fensterseite bietet schnellen Zugriff auf alle Programmfunktionen, auf die Ausführung von Aufgaben zur Virensuche oder zum Update, u.a.

Abbildung 4. Linke Seite des Fensters Computersicherheit

- Die rechte Seite des Fensters enthält Informationen über die auf der linken Seite ausgewählte Programmfunktion, erlaubt es, die ihre Parameter anzupassen, bietet Werkzeuge zum Ausführen von Aufgaben zur Virensuche, zum Update-Download, u.a.

Schutz-Center für Ihren Computer
Kaspersky PURE schützt den Computer vor Schadprogrammen, unerlaubtem Zugriff und gewährleistet sicheren Zugriff auf das lokale Netzwerk sowie das Internet.
Dateien und persönliche Daten
Dokumente und Media-Dateien. Zugriffsparameter auf die unterschiedlichen Ressourcen (Benutzernamen und Kennwörter), Daten für Kreditkarten u.a.
System und Programme
Auf Ihrem Computer installierte Programme und Objekte des Betriebssystems.
Arbeit im Netzwerk
Anzeige von Webseiten, Verwendung von Zahlungssystemen. E-Mail (Schutz vor Spam und Viren). Instant Messenger (ICQ, MSN u.a.)
Netzwerkmonitor
Insgesamt untersuchte Objekte: 523
Erkannte Bedrohungen: 0
Virus: 0
Trojanisches Programm: 0
Schädliches Tool: 0
Adware: 0
Anderes Programm: 0

Abbildung 5. Rechte Seite des Fensters Computersicherheit

Außerdem stehen folgende Links zur Verfügung:

- **Einstellungen** – in das Konfigurationsfenster für die Computersicherheit wechseln.
- **Quarantäne** – zur Arbeit mit Objekten, die in die Quarantäne verschoben wurden, wechseln.
- **Bericht** – zu einer Liste der Ereignisse, die bei der Arbeit des Programms eingetreten sind, wechseln.
- **Hilfe** – Hilfesystem für Kaspersky PURE öffnen.

BACKUP

Das Fenster **Backup** besteht aus zwei Teilen:

- Die linke Fensterseite bietet Zugriff auf folgende Funktionen: Verwaltung von Backup-Aufgaben und Backup-Speichern, Datenwiederherstellung.

- Auf der rechten Fensterseite befindet sich eine Liste mit Einstellungen für die im linken Bereich ausgewählte Funktion.

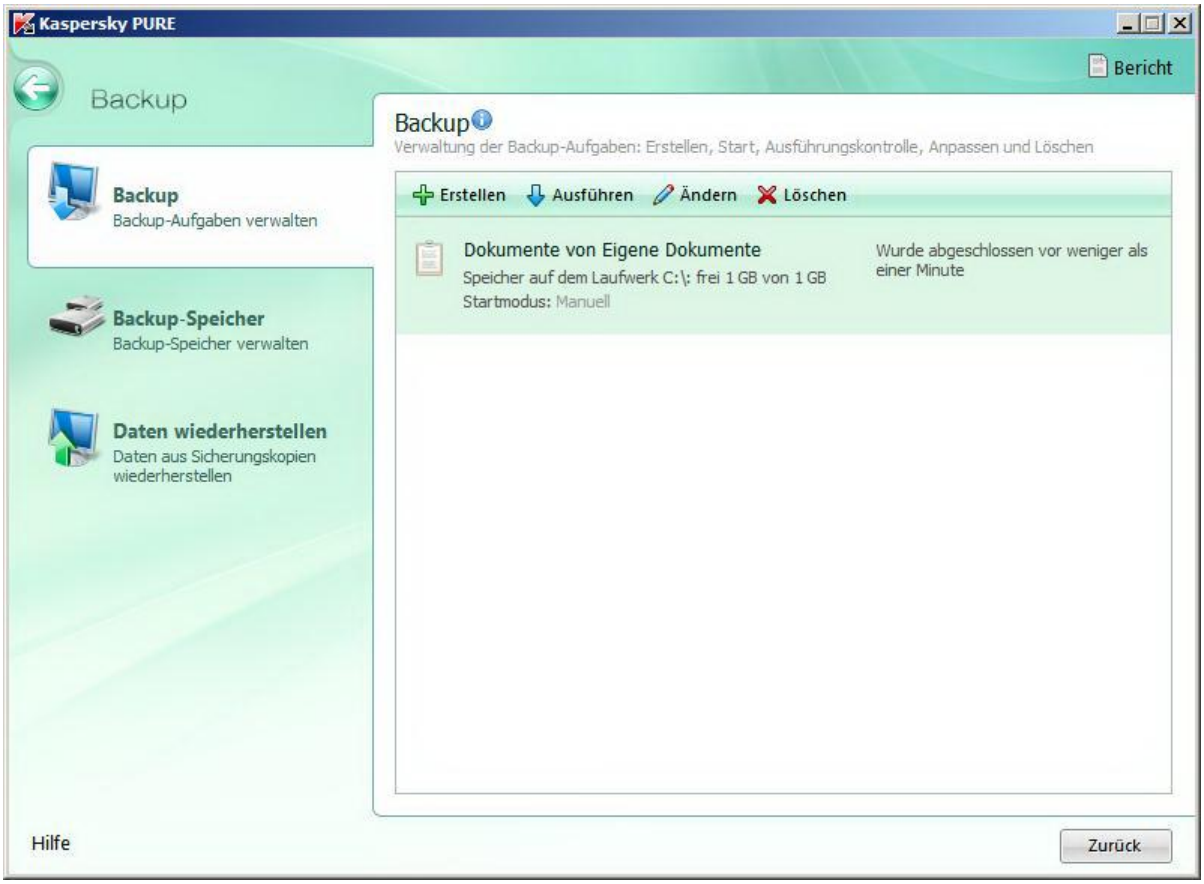


Abbildung 6. Hauptfenster des Moduls Backup

KINDERSICHERUNG

Das Fenster **Kindersicherung** besteht aus zwei Teilen:

- Die linke Fensterseite bietet Zugriff auf folgende Funktionen: Kontrolle für Computerbenutzer anpassen, Berichte anzeigen.

- Auf der rechten Fensterseite befindet sich eine Liste mit Einstellungen für die im linken Bereich ausgewählte Funktion.

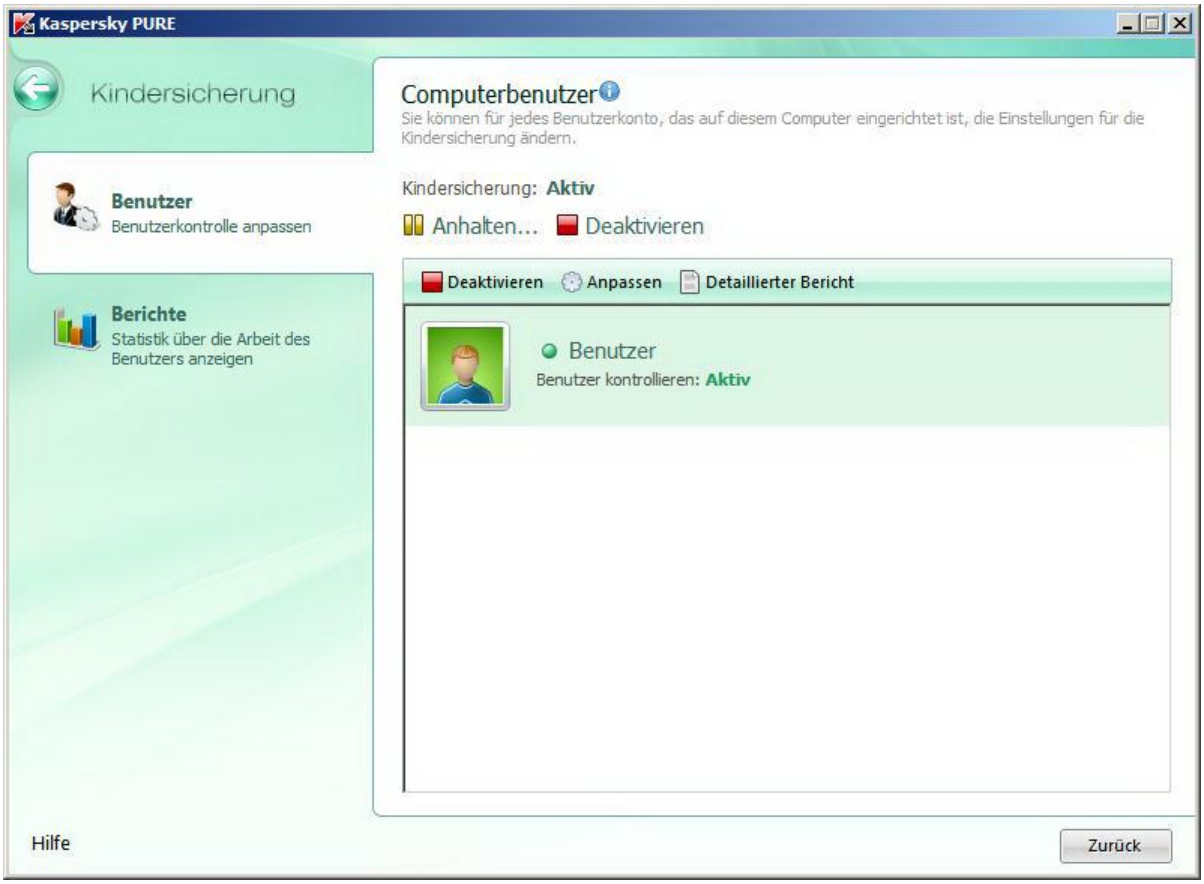


Abbildung 7. Hauptfenster des Moduls Kindersicherung

FENSTER VON PASSWORD MANAGER

Das Fenster **Password Manager** besteht aus drei Teilen:

- Schaltfläche zum Blockieren / Entsperren der Kennwort-Datenbank (s. S. 196).
- Schaltflächen für den schnellen Zugriff auf die wichtigsten Funktionen des Password Managers: Kennwort erstellen, Visitenkarte erstellen, Kennwort-Datenbank verwalten, Einstellungen für die Arbeit, das Erstellen und die Synchronisierung einer portablen Version des Password Managers anpassen (nicht verfügbar, wenn die Kennwort-Datenbank blockiert ist).
- Schaltfläche des Kennwort-Generators (s. S. 223).

Außerdem stehen folgende Schaltflächen und Links zur Verfügung:

- **Hilfe** - Hilfesystem des Password Managers öffnen.
- **Zurück** - in das Hauptfenster von Kaspersky PURE (s. S. 47) wechseln.

SYMBOL IM INFOBEREICH DER TASKLEISTE

Sofort nach dem Start von Password Manager erscheint sein Symbol im Infobereich der Taskleiste von Microsoft Windows.

In Abhängigkeit von der Situation besitzt das Symbol von Password Manager folgendes Aussehen:

- aktiv (grün) – Password Manager ist freigegeben. Der Zugriff auf persönliche Daten ist erlaubt.
- inaktiv (rot) – Password Manager es blockiert. Die persönlichen Daten sind nicht verfügbar.

Durch Klick auf das Symbol werden folgende Oberflächenelemente verfügbar:

- Kontextmenü (s. S. 53).
- Zeiger von Password Manager.

KONTEXTMENÜ VON PASSWORD MANAGER

Das Kontextmenü des Password Managers bietet Zugriff auf die wichtigsten Schutzaufgaben und enthält folgende Punkte:

- **Blockieren / Freigeben** – Verbot / Erlaubnis des Zugriffs auf Ihre persönlichen Daten.
- **Benutzerkonten** – schneller Zugriff auf häufig verwendete Benutzerkonten. Die Anzahl der Benutzerkonten in der Kennwort-Datenbank wird in Klammern genannt. Eine Liste der häufig verwendeten Benutzerkonten wird automatisch angelegt. Die Liste ist vorhanden, wenn festgelegt wurde, dass sie im Kontextmenü angezeigt werden soll (s. S. 212). Beim ersten Programmstart fehlt die Liste, weil noch kein Eintrag verwendet wurde.
- **Persönliche Notizen** – schneller Zugriff auf persönliche Notizen. Die Anzahl der persönlichen Notizen in der Kennwort-Datenbank wird in Klammern genannt.
- **Benutzerkonto hinzufügen** – Hinzufügen eines neuen Benutzerkontos zum Password Manager.
- **Password Manager** – Öffnen des Programmhauptfensters (s. S. 52).
- **Einstellungen** – Anpassen der Programmparameter.
- **Portable Version** - Assistent zum Erstellen einer portablen Version des Programms starten (s. S. 224).
- **Kennwort-Generator** – sichere Kennwörter erstellen (s. S. 223).
- **Hilfe** – Hilfesystem für das Programm öffnen.
- **Beenden** – Arbeit des Programms beenden (bei Auswahl dieses Menüpunkts wird das Programm aus dem Arbeitsspeicher des Computers entfernt).

Wenn das Programm nicht freigegeben ist, wird der Zugriff auf Ihre persönlichen Daten verboten. In diesem Fall stehen im Kontextmenü nur folgende Punkte zur Verfügung: **Freigeben**, **Kennwort-Generator**, **Hilfe** und **Beenden**.

➧ *Um das Kontextmenü zu öffnen,*

zeigen Sie im Infobereich der Taskleiste mit der Maus auf das Symbol des Password Managers und führen Sie einen Rechtsklick aus.

FENSTER DER KENNWORT-DATENBANK

Das Fenster der Kennwort-Datenbank besteht aus drei Teilen:

- Im oberen Fensterbereich können Funktionen von Password Manager ausgewählt und wichtige Aufgaben ausgeführt werden.

- Der mittlere Bereich des Fensters enthält eine Liste aller Benutzerkonten und anderen persönlichen Daten. Außerdem dient er der Verwaltung von persönlichen Informationen.

- Im unteren Fensterbereich befinden sich Links zur Verwaltung der Kennwort-Datenbank.

Außerdem können Sie die Suchzeile im oberen Fensterbereich verwenden. Mit der Suchzeile kann in der Kennwort-Datenbank mit Hilfe eines Schlüsselworts nach bestimmten Informationen gesucht werden.

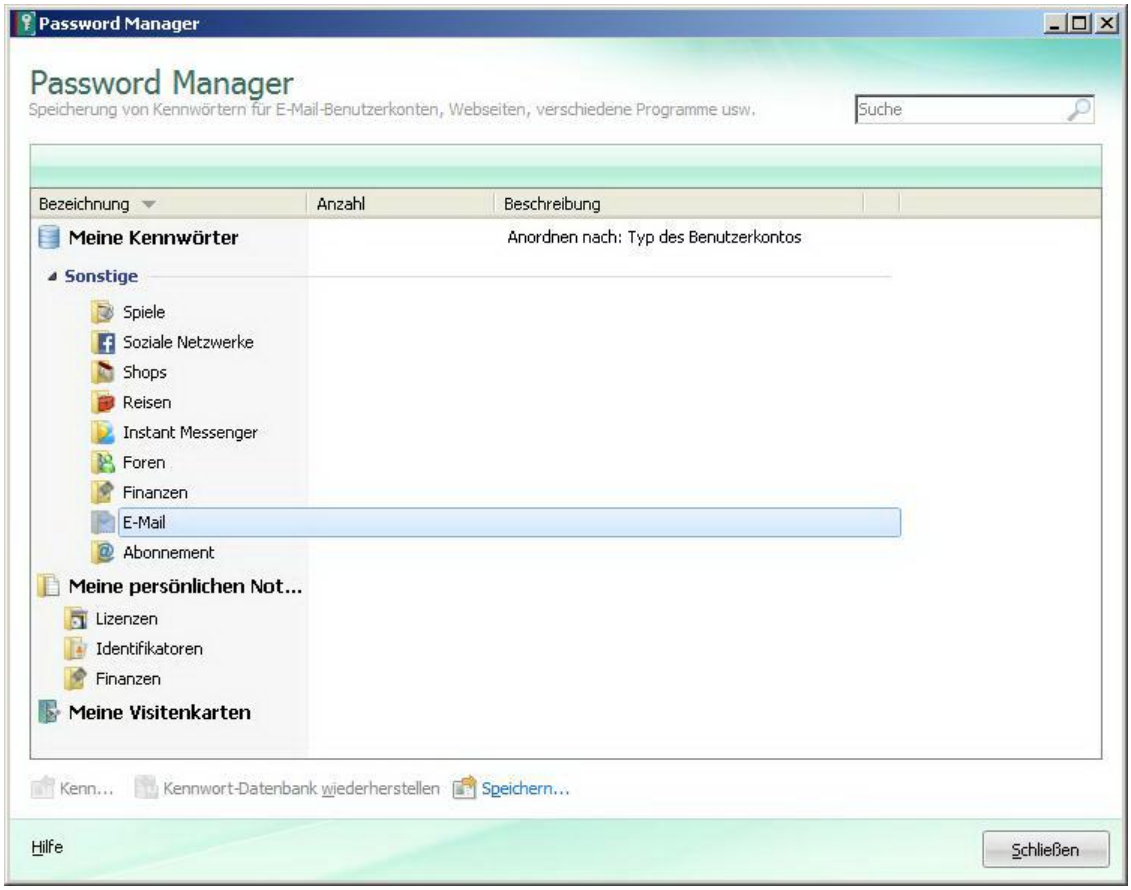


Abbildung 8. Fenster der Kennwort-Datenbank

KONFIGURATIONSFENSTER

Das Konfigurationsfenster von Password Manager kann auf eine der folgenden Arten geöffnet werden:

- aus dem Kontextmenü von Password Manager (s. S. 53) – Wählen Sie dazu im Kontextmenü von Password Manager den Punkt **Einstellungen**.

- aus dem Fenster von Kaspersky PURE **–** Klicken Sie dazu auf **Einstellungen**.

Das Konfigurationsfenster besteht aus zwei Teilen:

- Im linken Bereich des Fensters befindet sich eine Liste der Programmfunktionen.

- Auf der rechten Seite des Fensters steht eine Liste der Parameter für die ausgewählte Funktion, Aufgabe usw. zur Verfügung.

TITELLEISTEN-SCHALTFLÄCHE

Die Titelleisten-Schaltfläche erlaubt die Arbeit mit Ihren persönlichen Daten aus einem Programmfenster / einer Webseite. Die Schaltfläche befindet sich in der oberen rechten Ecke eines Programms.

Durch Klick auf die Titelleisten-Schaltfläche wird ein Menü mit der Liste der Benutzernamen geöffnet, die mit diesem Programm / mit dieser Webseite verknüpft sind. Bei Auswahl eines Benutzernamens füllt Password Manager auf Grundlage der Daten aus der Kennwort-Datenbank automatisch die Authentifizierungsfelder aus.

Die Titelleisten-Schaltfläche ist aktiv , wenn der Password Manager nicht blockiert ist (s. S. 196). Durch Klick auf die Schaltfläche gelangt man zu folgenden Aktionen:

- **Benutzerkonto hinzufügen** – Hinzufügen eines neuen Benutzerkontos.
- **Benutzerkonto ändern** – Hinzufügen eines Benutzernamens / Ändern eines aktivierten Benutzerkontos. Der Menüpunkt ist vorhanden, wenn das Benutzerkonto aktiviert wurde.
- **Internet-Benutzerkonten** – Anzeige einer Liste aller Benutzerkonten für das Internet und Start eines dieser Benutzerkonten. Die Anzahl der Benutzerkonten in der Kennwort-Datenbank wird in Klammern genannt.
- Liste der häufig verwendeten Benutzerkonten – Start eines Benutzerkontos aus der Liste. Die Liste wird aufgrund der Verwendungshäufigkeit von Benutzerkonten automatisch angelegt. Die Liste ist im Menü vorhanden, wenn zusätzlich ihre Anzeige angepasst wurde (s. S. 212).
- **Visitenkarten** – Anzeige einer Liste der erstellten Visitenkarten und Auswahl einer Visitenkarte für ein Anmeldeformular.
- **Hilfe** – Hilfe für das Programm.

Die Titelleisten-Schaltfläche ist inaktiv , wenn Password Manager blockiert ist. In diesem Fall ist es nicht möglich, durch Klick auf diese Schaltfläche zu dem genannten Aktionen zu gelangen. Die inaktive Schaltfläche wird in einem Programmfenster angezeigt, wenn zusätzlich die Parameter der Titelleisten-Schaltfläche angepasst wurden (s. S. 221).

ERWEITERUNGEN UND PLUG-INS

Password Manager besitzt Erweiterungskomponenten (Plug-ins), die in Programme integriert werden, für die eine Authentifizierung erforderlich ist. Sie können die Plug-ins für die von Ihnen benötigten Webbrowser selbst installieren. Installierte Plug-ins gewährleisten den Zugriff auf die Funktionen von Password Manager aus dem Interface eines Programms / Webbrowsers.

ZEIGER

Der Zeiger des Password Managers erlaubt es, ein Programm / eine Webseite schnell für das automatische Ausfüllen persönlicher Daten auszuwählen.

Gehen Sie folgendermaßen vor, um den Zeiger des Kennwort-Managers zu verwenden:

1. Führen Sie den Cursor auf das Symbol von Password Manager im Infobereich der Taskleiste und warten Sie einige Sekunden.
2. Sie den Zeiger von Password Manager in das entsprechende Programmfenster / Webseite. Password Manager ermittelt automatisch eine Aktion für das ausgewählte Programm / die Webseite.

PROGRAMMKONFIGURATIONSFENSTER

Das Konfigurationsfenster von Kaspersky PURE dient dazu, die allgemeinen Programmfunktionen, einzelne Schutzkomponenten, Untersuchungsaufgaben und Updateaufgaben anzupassen. Außerdem sind hier erweiterte Einstellungen (s. S. 84) für andere Aufgaben möglich.

Das Konfigurationsfenster besteht aus drei Teilen:

- Der obere Bereich enthält Kategorien für die Aufgaben und Funktionen von Kaspersky PURE.
- Der linke Fensterbereich bietet für die ausgewählte Kategorie Zugriff auf die Aufgaben und Funktionen von Kaspersky PURE.
- Auf der rechten Seite befindet sich eine Liste mit Einstellungen für die im linken Bereich ausgewählte Programmfunktion oder Aufgabe.

Das Konfigurationsfenster kann aus dem Hauptfenster (s. S. 47) oder aus dem Kontextmenü (s. S. 46) geöffnet werden. Um das Konfigurationsfenster zu öffnen, klicken Sie im oberen Bereich des Hauptfensters auf den Link **Einstellungen** oder wählen Sie den gleichnamigen Punkt im Kontextmenü des Programms.

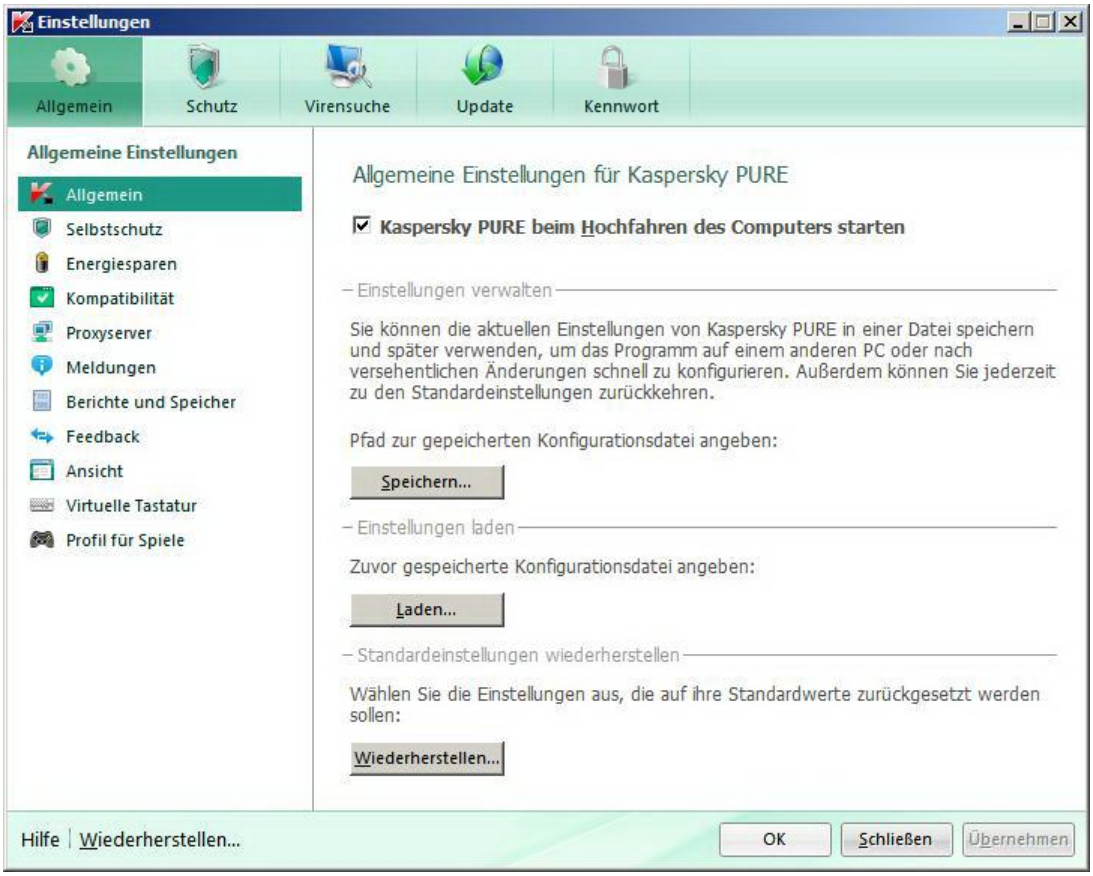


Abbildung 9. Kaspersky PURE anpassen

MELDUNGSFENSTER UND POPUPMELDUNGEN

Kaspersky PURE benachrichtigt Sie mit Hilfe von *Meldungsfenstern* und *Popupmeldungen*, die oberhalb des Programmsymbols im Infobereich der Taskleiste angezeigt werden, über wichtige Ereignisse, die während seiner Ausführung eintreten.

Kaspersky PURE zeigt die *Meldungsfenster* immer dann auf dem Bildschirm an, wenn verschiedene Reaktionen auf das Ereignis möglich sind. So können Sie beispielsweise bei Erkennen eines schädlichen Objekts den Zugriff darauf blockieren, dieses löschen oder versuchen, es zu desinfizieren. Das Programm stellt Ihnen die entsprechenden Optionen zu Auswahl. Das Meldungsfenster wird erst dann wieder geschlossen, wenn Sie eine der vorgeschlagenen Optionen ausgewählt haben.

Abbildung 10. Fenster Meldungen

Kaspersky PURE zeigt *Popupfenster* auf dem Bildschirm an, um Sie über Ereignisse zu informieren, die keine Entscheidung Ihrerseits über die weitere Vorgehensweise erfordern. Einige Popupmeldungen beinhalten Links, mit deren Hilfe Sie eine vorgeschlagene Aktion ausführen können (z. B. ein Datenbankupdate starten oder zur Programmaktivierung wechseln). Popupmeldungen verschwinden nach kurzer Zeit automatisch vom Bildschirm.

Kaspersky PURE
Der Schutz wurde deaktiviert
Schutz fortsetzen
Das von Ihnen verwendete Programm wurde nicht aktiviert.
Bitte aktivieren Sie das Programm.

Abbildung 11. Popupmeldung

In Abhängigkeit davon, welche Relevanz das Ereignis für die Computersicherheit besitzt, sind folgende Arten von Meldungen möglich:

- Kritische Meldungen informieren über die Ereignisse, die vorrangige Priorität für die Computersicherheit aufweisen. Beispiele: "Ein schädliches Objekt wurde gefunden" oder "Im System wurde eine gefährliche Aktivität erkannt". Benachrichtigungsfenster und Popupmeldungen dieses Typs werden rot angezeigt.

- Wichtige Meldungen informieren über die Ereignisse, die für die Computersicherheit potentiell wichtig sind. Beispiele: "Ein möglicherweise infiziertes Objekt wurde gefunden" oder "Im System wurde verdächtige Aktivität erkannt". Benachrichtigungsfenster und Popupmeldungen dieses Typs werden gelb angezeigt.

- Informative Meldungen informieren über die Ereignisse, die vom Standpunkt der Sicherheit aus keine vorrangige Priorität besitzen. Benachrichtigungsfenster und Popupmeldungen dieses Typs werden grün angezeigt.

PROGRAMM STARTEN UND BEENDEN

Kaspersky PURE wird nach der Installation automatisch gestartet. In der Grundeinstellung ist vorgesehen, dass das Programm künftig beim Hochfahren des Betriebssystems automatisch gestartet wird.

IN DIESEM ABSCHNITT

Automatischen Start aktivieren und deaktivieren 58

Programm manuell starten und beenden 58

AUTOMATISCHEN START AKTIVIEREN UND DEAKTIVIEREN

Unter dem automatischen Programmstart wird hier der Start von Kaspersky PURE verstanden, der ohne Ihr Zutun sofort nach dem Hochfahren des Betriebssystems ausgeführt wird. Diese Startvariante gilt als Standard.

- *Geben Sie folgendermaßen vor, um den automatischen Start des Programms zu deaktivieren:*

  1. Öffnen Sie das Programmhauptfenster.
  2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
  3. Wählen Sie auf der linken Fensterseite im Abschnitt **Allgemeine Einstellungen** den Abschnitt **Allgemein**.
  4. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Kaspersky PURE beim Hochfahren des Computers starten**.

PROGRAMM MANUELL STARTEN UND BEENDEN

Kaspersky Lab warnt davor, Kaspersky PURE zu beenden, da andernfalls der Computer und Ihre persönlichen Daten bedroht sind. Sollte es trotzdem notwendig sein, so wird empfohlen, den Computerschutz nur anzuhalten (s. S. 61), ohne das Programm zu beenden.

Kaspersky PURE muss manuell gestartet werden, falls Sie den automatischen Programmstart (s. S. 58) deaktiviert haben.

- *Um das Programm manuell zu starten,*

  wählen Sie im **Startmenü** den Punkt **Programme** → **Kaspersky PURE** → **Kaspersky PURE**.

- *Um die Arbeit des Programms zu beenden,*

  öffnen Sie durch Rechtsklick das Kontextmenü des Programmsymbols, das sich im Infobereich der Taskleiste befindet, und wählen Sie den Punkt **Beenden**.

STATUS DES SCHUTZES FÜR EIN HEIMNETZWERK

Dieser Abschnitt informiert darüber, wie ermittelt wird, ob das Heimnetzwerk im Augenblick sicher ist oder ob seine Sicherheit bedroht ist. Außerdem wird die Neutralisierung von vorhandenen Bedrohungen beschrieben.

Hier finden Sie Informationen darüber, wie der Schutz während der Arbeit von Kaspersky PURE aktiviert, deaktiviert und vorübergehend angehalten werden kann.

PROBLEME IM SCHUTZ DIAGNOSTIZIEREN UND BEHEBEN

Probleme im Schutz des Computers werden durch den Indikator signalisiert, der sich im oberen Bereich des Hauptfensters von Kaspersky PURE befindet. Der Indikator ändert seine Farbe in Abhängigkeit vom Schutzstatus des Computers: Die Farbe Grün bedeutet, dass der Computer sicher ist. Gelb signalisiert, dass der Schutz Probleme aufweist, und Rot warnt vor einer ernsthaften Bedrohung für die Computersicherheit. Probleme und Sicherheitsrisiken sollten umgehend behoben werden.

Durch Klick auf die Schaltfläche **Korrigieren** wird das Fenster **Genereller Schutzstatus** geöffnet werden (s. Abb. unten). Es enthält ausführliche Angaben zum Schutzstatus des Computers und bietet Aktionsvarianten zum Beheben von Problemen und Gefahren.

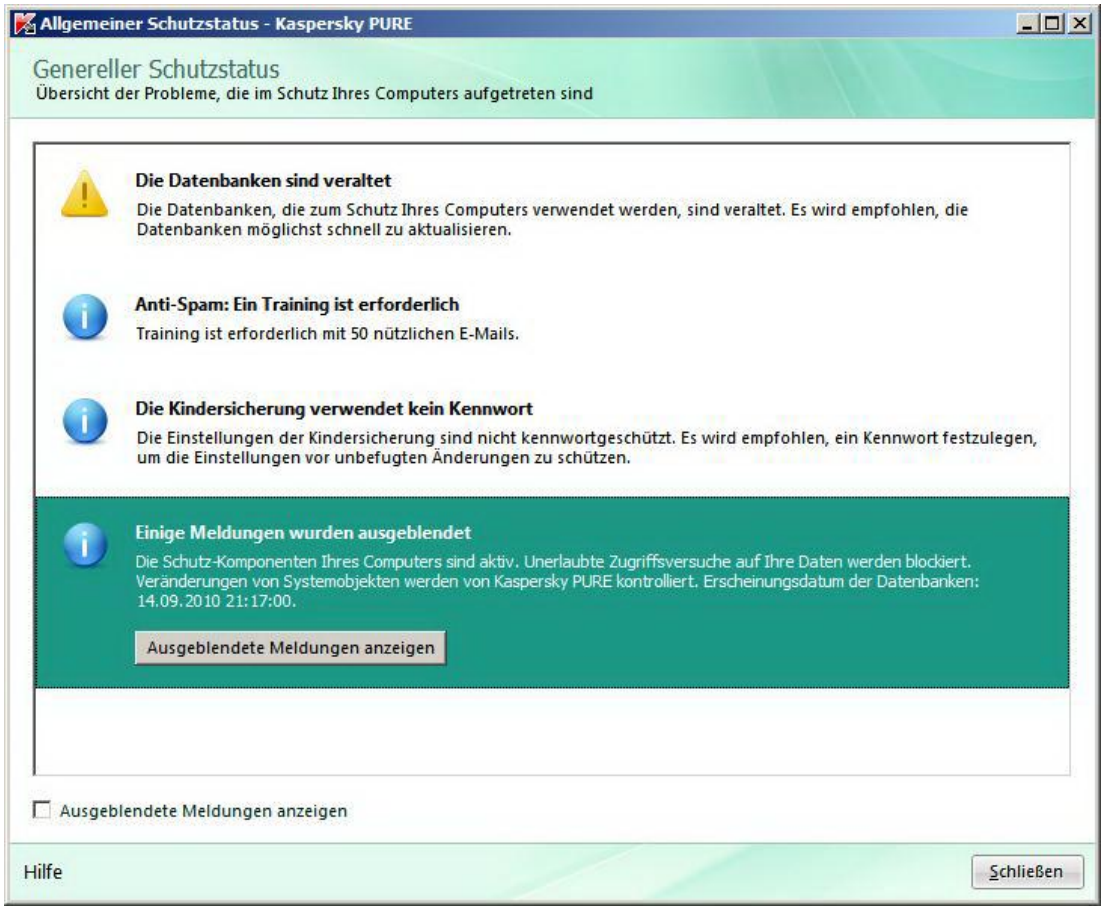

Allgemeiner Schutzstatus - Kaspersky PURE
Genereller Schutzstatus
Übersicht der Probleme, die im Schutz Ihres Computers aufgetreten sind
Die Datenbanken sind veraltet
Die Datenbanken, die zum Schutz Ihres Computers verwendet werden, sind veraltet. Es wird empfohlen, die Datenbanken möglichst schnell zu aktualisieren.
Anti-Spam: Ein Training ist erforderlich
Training ist erforderlich mit 50 nützlichen E-Mails.
Die Kindersicherung verwendet kein Kennwort
Die Einstellungen der Kindersicherung sind nicht kennwortgeschützt. Es wird empfohlen, ein Kennwort festzulegen, um die Einstellungen vor unbefugten Änderungen zu schützen.
Einige Meldungen wurden ausgeblendet
Die Schutz-Komponenten Ihres Computers sind aktiv. Unerlaubte Zugriffsversuche auf Ihre Daten werden blockiert. Veränderungen von Systemobjekten werden von Kaspersky PURE kontrolliert. Erscheinungsdatum der Datenbanken: 14.09.2010 21:17:00.
Ausgeblendete Meldungen anzeigen
Ausgeblendete Meldungen anzeigen
Hilfe
Schließen

Abbildung 12. Fenster Genereller Schutzstatus

Das Fenster enthält eine Liste der im Schutz vorhandenen Probleme. Dazu zählen auch Probleme, die auf Abweichungen von der optimalen Programmfunktion zurückgehen (z.B. veraltete Datenbanken). Zum Beheben von

Problemen und Bedrohungen werden folgende Aktionsvarianten angeboten:

- Sofort beheben. Durch Klick auf die Schaltfläche mit der vorgeschlagenen Aktionsvariante können Sie direkt zur Problembehebung übergehen. Diese Aktion gilt als empfohlen.

- Behebung aufschieben. Wenn das sofortige Beheben eines Problems aufgrund bestimmter Umstände nicht möglich ist, kann diese Aktion aufgeschoben werden und Sie können später dazu zurückkehren. Klicken Sie dazu auf **Meldung ausblenden**.

  Beachten Sie, dass es für kritische Probleme nicht vorgesehen ist, das Beheben aufzuschieben. Zu diesen Problemen gehören beispielsweise die Existenz nicht neutralisierter schädlicher Objekte, Funktionsstörungen einer oder mehrerer Komponenten und beschädigte Programmdateien.

Um Meldungen, die zuvor ausgeblendet waren, erneut in der allgemeinen Liste anzuzeigen, klicken Sie im Listenelement **Einige Meldungen wurden ausgeblendet** auf **Ausgeblendete Meldungen anzeigen**.

Das Schutzniveau des Heimnetzwerks kann von einem Administratorarbeitsplatz aus mit Hilfe der Verwaltung (s. Abschnitt "Wie der Schutzstatus für ein Heimnetzwerk ferngesteuert geprüft wird" auf S. 69) analysiert werden.

COMPUTERSCHUTZ AKTIVIEREN/DEAKTIVIEREN

Kaspersky PURE wird in der Grundeinstellung automatisch beim Start des Betriebssystems gestartet und schützt Ihren Computer während der gesamten Sitzung. Alle Schutzkomponenten sind aktiv.

Sie können den Schutz, der von Kaspersky PURE gewährleistet wird, vollständig oder teilweise deaktivieren.

Die Kaspersky-Lab-Spezialisten **warnen ausdrücklich davor, den Schutz zu deaktivieren**, weil dies zur Infektion Ihres Computers und zu Datenverlust führen kann.

Wenn der Schutz deaktiviert wird, wird die Arbeit aller Komponenten beendet. Darüber informieren folgende Merkmale:

- inaktive (graues) Symbol von Kaspersky PURE (im Abschnitt "Symbol im Infobereich der Taskleiste" auf S. 45) im Infobereich der Taskleiste.

- rote Farbe des Sicherheitsindikators

Beachten Sie, dass der Schutz hier ausdrücklich im Kontext der Schutzkomponenten beschrieben wird. Das Deaktivieren oder Anhalten von Schutzkomponenten übt keinen Einfluss auf die Ausführung von Aufgaben zur Virensuche und zum Update für Kaspersky PURE aus.

Gehen Sie folgendermaßen vor, um den Schutz vollständig auszuschalten:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.
2. Klicken Sie im oberen Bereich des folgenden Fensters auf den Link **Einstellungen**.
3. Wählen Sie im folgenden Fenster den Abschnitt **Schutz-Center**.
4. Deaktivieren Sie das Kontrollkästchen **Schutz aktivieren**.

Gehen Sie folgendermaßen vor, um eine Schutzkomponente zu aktivieren/deaktivieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.

   Das Fenster **Computersicherheit** wird geöffnet.

2. Wählen Sie im linken Fensterbereich den Abschnitt **Schutz-Center** aus und klicken Sie im rechten Fensterbereich auf die Schaltfläche mit dem Namen der zu schützenden Kategorie.

3. Aktivieren / deaktivieren Sie im folgenden Fenster **Schutzkomponenten** die entsprechende Schutzkomponente durch Klick auf das Statussymbol rechts vom Namen der Komponente.

SCHUTZ ANHALTEN

Das Anhalten des Schutzes bedeutet, dass alle Komponenten für einen bestimmten Zeitraum ausgeschaltet werden.

Durch das vorübergehende Deaktivieren wird die Arbeit aller Schutzkomponenten angehalten. Darüber informieren:

- Das inaktive (graue) (s. Abschnitt "Symbol im Infobereich der Taskleiste" auf S. 45) im Infobereich der Taskleiste.
- Rote Farbe von Statussymbol und Leiste im Fenster der Computersicherheit.

Wenn im Augenblick, als der Schutz beendet wurde, auf dem Computer Netzwerkverbindungen vorhanden waren, erscheint auf dem Bildschirm eine Meldung darüber, dass diese Verbindungen getrennt werden.

Gehen Sie folgendermaßen vor, um den Computerschutz anzuhalten:

1. Im Kontextmenü (s. Abschnitt "Kontextmenü" auf S. 46) des Programms wählen Sie den Punkt **Schutz anhalten**.
2. Wählen Sie im folgenden Fenster **Schutz anhalten** den Zeitraum, nach dem der Schutz wieder aktiviert werden soll:
   - **Anhalten für <Zeitintervall> –** Der Schutz wird nach Ablauf des festgelegten Zeitraums wieder aktiviert. Wählen Sie in der Dropdown-Liste einen Wert für den Zeitraum.
   - **Anhalten bis zum Neustart –** Der Schutz wird nach dem Neustart des Programms oder des Systems aktiviert (unter der Bedingung, dass der Modus zum Start von Kaspersky PURE beim Hochfahren des Systems aktiviert ist).
   - **Anhalten –** Der Schutz wird erst dann wieder aktiviert, wenn Sie ihn starten. Wählen Sie den Punkt **Schutz fortsetzen** im Kontextmenü des Programms, um den Schutz zu aktivieren.

INTERAKTIVEN SCHUTZMODUS VERWENDEN

Kaspersky PURE bietet zwei Modi für die Kooperation mit dem Benutzer:

- *Interaktiver Schutzmodus*. Kaspersky PURE benachrichtigt den Benutzer über alle gefährlichen und verdächtigen Ereignisse im System. In diesem Modus muss der selbständig entscheiden, ob bestimmte Aktionen erlaubt oder verboten werden sollen.
- *Automatischer Schutzmodus*. Kaspersky PURE führt automatisch die von den Kaspersky-Lab-Experten empfohlene Aktion aus, wenn gefährliche Ereignisse eintreten.

Gehen Sie folgendermaßen vor, um einen Schutzmodus zu wählen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite unter **Schutz-Center** den Abschnitt **Allgemeine Einstellungen**.
4. Deaktivieren oder aktivieren Sie im rechten Fensterbereich im Block **Interaktiver Modus** die Kontrollkästchen für den entsprechenden Schutzmodus:
   - um den interaktiven Schutzmodus zu wählen, deaktivieren Sie das Kontrollkästchen **Aktion automatisch wählen**.

- um den automatischen Schutzmodus zu wählen, aktivieren Sie das Kontrollkästchen **Aktion automatisch wählen**.

Damit verdächtige Objekte bei der Arbeit im automatischen Modus nicht gelöscht werden, aktivieren Sie das Kontrollkästchen **Verdächtige Objekte nicht löschen**.

LÖSUNGEN FÜR TYPISCHE AUFGABEN

Dieser Abschnitt bietet eine Anleitung für die grundlegenden Aufgaben des Programms, die der Benutzer am häufigsten benötigt.

IN DIESEM ABSCHNITT

Wie das Programm aktiviert wird. ... 63

Lizenzerwerb oder -verlängerung ... 64

Was tun, wenn das Programm Meldungen anzeigt? ... 65

Aktualisierung von Programmdatenbanken und -modulen ... 65

Wie wichtige Computerbereiche auf Viren untersucht werden. ... 65

Untersuchung von Dateien, Ordnern, Laufwerken und anderen Objekten auf Viren ... 66

Wie eine vollständige Virenuntersuchung des Computers ausgeführt wird. ... 68

Wie der Computer auf Schwachstellen untersucht wird. ... 68

Wie der Schutzstatus für ein Heimnetzwerk ferngesteuert geprüft wird ... 69

Wie Ihre persönlichen Daten vor Diebstahl geschützt werden. ... 70

Was tun, wenn Sie vermuten, dass ein Objekt von einem Virus infiziert ist? ... 73

Wie ein Objekt wiederhergestellt wird, das vom Programm gelöscht oder desinfiziert wurde. ... 74

Was tun, wenn Sie vermuten, dass Ihr Computer infiziert ist? ... 74

Wie Sicherungskopien Ihrer Daten angelegt werden ... 76

Wie der Zugriff auf die Einstellungen von Kaspersky PURE eingeschränkt wird ... 77

Wie die Verwendung des Computers und Internets für verschiedene Benutzer eingeschränkt wird ... 78

Wie eine Notfall-CD erstellt und verwendet wird. ... 78

Wie mit einer großen Anzahl von Spam-Mails verfahren wird? ... 80

Wie ein Bericht über den Computerschutz geöffnet wird ... 82

Wie die Standardeinstellungen des Programms wiederhergestellt werden ... 82

Wie die Programmeinstellungen auf einen anderen Computer übertragen werden ... 83

WIE DAS PROGRAMM AKTIVIERT WIRD.

Durch die *Aktivierung* erlangt die Lizenz für die Nutzung der Vollversion des Programms ihre Gültigkeit für den entsprechenden Zeitraum.

Wenn Sie das Programm nicht im Verlauf der Installation aktiviert haben (s. S. 35), können Sie dies später nachholen. Falls eine Programmaktivierung notwendig ist, werden Sie von Kaspersky PURE durch entsprechende Meldungen im Infobereich der Taskleiste daran erinnert.

Gehen Sie folgendermaßen vor, um den Aktivierungsassistenten für Kaspersky PURE zu starten:

- Klicken Sie im Meldungsfenster von Kaspersky PURE, das im Infobereich der Taskleiste erscheint, auf den Link **Bitte aktivieren Sie das Programm**.
- Verwenden Sie im unteren Bereich des Programmhauptfensters den Link **Lizenz**. Klicken Sie im folgenden Fenster **Lizenzen verwalten** auf **Programm mit neuer Lizenz aktivieren**.

Details zu den einzelnen Schritte des Assistenten:

Schritt 1. Lizenztyp wählen und Aktivierungscode eingeben

Vergewissern Sie sich, dass im Assistentenfenster die Variante **Kommerzielle Version aktivieren** gewählt wurde, geben Sie den Aktivierungscode (s. Abschnitt "Über den Aktivierungscode" auf S. 43) im entsprechenden Feld ein und klicken Sie auf **Weiter**.

Schritt 2. Aktivierungsanfrage

Im ersten Schritt sendet der Assistent eine Anfrage zur Aktivierung der kommerziellen Programmversion an den Aktivierungsserver. Der Assistent geht nach erfolgreicher Anfrage automatisch zum nächsten Schritt.

Schritt 3. Assistent abschließen

Dieses Fenster des Assistenten informiert über die Aktivierungsergebnisse: Typ und Gültigkeitsdauer der verwendeten Lizenz.

Klicken Sie auf die Schaltfläche **Beenden**, um den Assistenten abzuschließen.

LIZENZERWERB ODER -VERLÄNGERUNG

Wenn Sie Kaspersky PURE installiert haben und keine Lizenz besitzen, können Sie die Lizenz nach der Programminstallation erwerben. Wenn die Gültigkeit einer Lizenz bald abläuft, können Sie diese verlängern. Sie erhalten einen Aktivierungscode, mit dem das Programm aktiviert werden muss.

Gehen Sie folgendermaßen vor, um eine Lizenz zu erwerben:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Lizenz kaufen**.

   Die Webseite des Online-Shops wird geöffnet. Dort können Sie eine Lizenz erwerben.

Gehen Sie folgendermaßen vor, um die Gültigkeitsdauer einer Lizenz zu verlängern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie unten im Hauptfenster auf den Link **Lizenz**.

   Das Fenster **Lizenzen verwalten** wird geöffnet.

2. Klicken Sie auf die Schaltfläche **Gültigkeitsdauer der Lizenz verlängern**.

   Eine Webseite zur Lizenzaktualisierung wird geöffnet. Dort können Sie die Gültigkeitsdauer Ihrer Lizenz verlängern.

WAS TUN, WENN DAS PROGRAMM MELDUNGEN ANZEIGT?

Meldungen, die das Programm im Infobereich der Taskleiste anzeigt, informieren über Ereignisse bei der Arbeit des Programms und erfordern Ihre Aufmerksamkeit. In Abhängigkeit von der Priorität eines Ereignisses sind folgende Arten von Meldungen möglich:

- Kritische Meldungen informieren über die Ereignisse, die vorrangige Priorität für die Computersicherheit aufweisen. Beispiele: "Ein schädliches Objekt wurde gefunden" oder "Im System wurde eine gefährliche Aktivität erkannt". Benachrichtigungsfenster und Popupmeldungen dieses Typs werden rot angezeigt.

- Wichtige Meldungen informieren über die Ereignisse, die für die Computersicherheit potentiell wichtig sind. Beispiele: "Ein möglicherweise infiziertes Objekt wurde gefunden" oder "Im System wurde verdächtige Aktivität erkannt". Benachrichtigungsfenster und Popupmeldungen dieses Typs werden gelb angezeigt.

- Informative Meldungen informieren über die Ereignisse, die vom Standpunkt der Sicherheit aus keine vorrangige Priorität besitzen. Benachrichtigungsfenster und Popupmeldungen dieses Typs werden grün angezeigt.

Erscheint eine solche Benachrichtigung auf dem Bildschirm, muss eine der vorgegebenen Varianten für die weitere Vorgehensweise ausgewählt werden. Als optimal gilt die von Kaspersky Lab empfohlene Variante.

AKTUALISIERUNG VON PROGRAMMDATENBANKEN UND -MODULEN

Kaspersky PURE überprüft in der Grundeinstellung automatisch, ob auf den Kaspersky-Lab-Updateservern neue Updates vorhanden sind. Wenn auf dem Server neue Updates vorhanden sind, führt Kaspersky PURE im Hintergrundmodus den Download und die Installation der Updates durch. Sie können das Update von Kaspersky PURE jederzeit starten.

Um Updates von den Kaspersky-Lab-Servern herunterzuladen, ist eine Internetverbindung erforderlich.

Um den aktuellen Zustand Ihres Computerschutzes zu gewährleisten, wird empfohlen, Kaspersky PURE sofort nach der Installation zu aktualisieren.

Um das Update aus dem Kontextmenü zu starten,

wählen Sie im Kontextmenü des Programmsymbols den Punkt **Update**.

Gehen Sie folgendermaßen vor, um das Update aus dem Hauptfenster zu starten:

Öffnen Sie das Programmhauptfenster, klicken Sie im Block **Computersicherheit** auf Schneller Aufgabenstart und wählen Sie den Punkt **Datenbank-Update** ausführen.

WIE WICHTIGE COMPUTERBEREICHE AUF VIREN UNTERSUCHT WERDEN.

Die schnelle Untersuchung umfasst die Untersuchung von Objekten, die während des Hochfahrens des Betriebssystems geladen werden, sowie die Untersuchung des Arbeitsspeichers, der Laufwerksbootsektoren und der vom Benutzer hinzugefügten Objekte. Eine schnelle Untersuchung wird automatisch bei der Installation von Kaspersky PURE ausgeführt.

Sie können die Aufgabe zur schnellen Untersuchung auf folgende Weise starten:

- mit einer zuvor hergestellten Verknüpfung (s. S. 93).

- aus dem Programmhauptfenster (s. Abschnitt "Hauptfenster von Kaspersky PURE" auf S. 47)

Gehen Sie folgendermaßen vor, um die Aufgabe zur schnellen Untersuchung mit Hilfe einer Verknüpfung zu starten:

1. Öffnen Sie das Fenster von Microsoft Windows Explorer und öffnen Sie den Ordner, in dem Sie die Verknüpfung erstellt haben.
2. Starten Sie die Untersuchung durch Doppelklick auf die Verknüpfung.

Gehen Sie folgendermaßen vor, um die Aufgabe zur schnellen Untersuchung aus dem Programmhauptfenster zu starten:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.
2. Wählen Sie im linken Bereich den Abschnitt **Untersuchung**.
3. Klicken Sie auf der rechten Fensterseite auf **Schnelle Untersuchung ausführen**.

   Die Informationen über die laufende Untersuchung werden angezeigt:

   - im Block **Computersicherheit** des Programmhauptfensters im Feld **Untersuchung**.
   - im Abschnitt **Untersuchung** des Fensters **Computersicherheit**, im Block **Schnelle Untersuchung abbrechen**.
   - im Fenster **Schnelle Untersuchung**, das mit dem Link **Ende** im Block **Schnelle Untersuchung abbrechen** geöffnet wird.
   - im Kontextmenü des Programmsymbols (s. S. 46).

Gehen Sie wie folgt vor, um die schnelle Untersuchung abzubrechen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.
2. Wählen Sie im linken Bereich den Abschnitt **Untersuchung**.
3. Klicken Sie auf der rechten Fensterseite auf **Schnelle Untersuchung abbrechen**.

UNTERSUCHUNG VON DATEIEN, ORDNERN, LAUFWERKEN UND ANDEREN OBJEKTEN AUF VIREN

Ein bestimmtes Objekt kann folgendermaßen auf Viren untersucht werden:

- mit Hilfe des Kontextmenüs für ein Objekt
- aus dem Programmhauptfenster (s. Hauptfenster von Kaspersky PURE" auf S. 47)

Gehen Sie folgendermaßen vor, um eine Untersuchungsaufgabe aus dem Kontextmenü eines Objekts zu starten:

1. Öffnen Sie das Fenster von Microsoft Windows Explorer und gehen Sie in den Ordner, in dem sich das Untersuchungsobjekt befindet.
2. Öffnen Sie durch Rechtsklick das Kontextmenü für das Objekt (s. Abb. unten) und wählen Sie den Punkt **Auf Viren untersuchen**.

Der Vorgang und das Ergebnis der Aufgabenausführung werden im folgenden Fenster **Auf Viren untersuchen** angezeigt.

Abbildung 13. Kontextmenü für ein Objekt in Microsoft Windows

Gehen Sie folgendermaßen vor, um die Untersuchung eines Objekts aus dem Programmhauptfenster zu starten:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.
2. Wählen Sie im linken Bereich den Abschnitt **Untersuchung**.
3. Klicken Sie auf der rechten Fensterseite im Block **Untersuchung von Objekten ausführen** auf den Link **Hinzufügen**.
4. Geben Sie im folgenden Fenster **Untersuchungsobjekt auswählen** den Ort des Objekts an, das Sie auf Viren untersuchen möchten.
5. Aktivieren Sie im Block **Untersuchung von Objekten ausführen** die Kontrollkästchen für die Objekte, die untersucht werden sollen.
6. Klicken Sie auf **Untersuchung von Objekten ausführen**.

   Die Informationen über die laufende Untersuchung werden angezeigt:

   - im Block **Computersicherheit** des Programmhauptfensters im Feld **Untersuchung**.
   - im Abschnitt **Untersuchung** des Fensters **Computersicherheit**, im Block **Untersuchung von Objekten abbrechen**.
   - im Fenster **Untersuchung von Objekten**, das mit dem Link **Ende** im Block **Untersuchung von Objekten abbrechen** geöffnet wird.
   - im Kontextmenü des Programmsymbols (s. S. 46).

Gehen Sie folgendermaßen vor, um die Objektuntersuchung anzuhalten:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.
2. Wählen Sie im linken Bereich den Abschnitt **Untersuchung**.
3. Klicken Sie auf der rechten Fensterseite auf **Untersuchung von Objekten abbrechen**.

WIE EINE VOLLSTÄNDIGE VIRENUNTERSUCHUNG DES COMPUTERS AUSGEFÜHRT WIRD.

Die Aufgabe zur vollständigen Virenuntersuchung kann folgendermaßen gestartet werden:

- mit einer zuvor hergestellten Verknüpfung (s. S. 93).
- aus dem Programmhauptfenster (s. Hauptfenster von Kaspersky PURE" auf S. 47)

Gehen Sie folgendermaßen vor, um die Aufgabe zur vollständigen Untersuchung mit Hilfe einer Verknüpfung zu starten:

1. Öffnen Sie das Fenster von Microsoft Windows Explorer und öffnen Sie den Ordner, in dem Sie die Verknüpfung erstellt haben.
2. Starten Sie die Untersuchung durch Doppelklick auf die Verknüpfung.

Gehen Sie folgendermaßen vor, um die Aufgabe zur vollständigen Untersuchung aus dem Programmhauptfenster zu starten:

Öffnen Sie das Programmhauptfenster, klicken Sie im Block **Computersicherheit** auf **Schneller Aufgabenstart** und wählen Sie den Punkt **Vollständige Untersuchung** ausführen.

WIE DER COMPUTER AUF SCHWACHSTELLEN UNTERSUCHT WIRD.

Schwachstellen sind Teile eines Programmcodes, den Angreifer für ihre Ziele nutzen können, um beispielsweise Daten zu kopieren, die von Programmen mit ungeschütztem Code verwendet werden. Die Untersuchung Ihres Computers auf potentielle Schwachstellen erlaubt es, solche "Schwachpunkte" im Schutz des Rechners zu finden. Erkannte Schwachstellen sollten beseitigt werden.

Sie können die Schwachstellensuche auf folgende Weise starten:

- aus dem Programmhauptfenster (s. Abschnitt Hauptfenster von Kaspersky PURE" auf S. 47)
- mit Hilfe einer zuvor erstellten Verknüpfung

Gehen Sie folgendermaßen vor, um eine Aufgabe mit Hilfe einer Verknüpfung zu starten:

1. Öffnen Sie das Fenster von Microsoft Windows Explorer und öffnen Sie den Ordner, in dem Sie die Verknüpfung erstellt haben.
2. Starten Sie die Aufgabe zur Schwachstellensuche durch Doppelklick auf die Verknüpfung.

   Informationen über die Aufgabenausführung werden im geöffneten Fenster **Schwachstellensuche** angezeigt.

Gehen Sie folgendermaßen vor, um die Aufgabe aus dem Programmhauptfenster zu starten:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.
2. Wählen Sie im linken Bereich den Abschnitt **Untersuchung**.
3. Klicken Sie auf **Fenster zur Schwachstellensuche öffnen**.
4. Klicken Sie im folgenden Fenster auf **Schwachstellensuche starten**.

Informationen über die Aufgabenausführung werden im geöffneten Fenster **Schwachstellensuche** angezeigt. Die gefundenen Schwachstellen werden auf den Registerkarten **Systemschwachstellen** und **Programme mit Schwachstellen** genannt.

WIE DER SCHUTZSTATUS FÜR EIN HEIMNETZWERK FERNGESTEUERT GEPRÜFT WIRD

Um das Programm Kaspersky PURE von einem Administratorarbeitsplatz aus auf den Computern eines Heimnetzwerks fernzuverwalten, dienen die Funktionen der Verwaltung (s. S. 191).

Sie können das generelle Schutzniveau des Heimnetzwerks analysieren, oder eine Liste der auf einem bestimmten Netzwerkcomputer vorliegenden Probleme anzeigen und bestimmte Probleme ferngesteuert zu beheben.

- *Gehen Sie folgendermaßen vor, um ausführliche Informationen über im Netzwerkschutz vorliegende Probleme und entsprechende Lösungsvorschläge zu erhalten:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im unteren Fensterbereich auf **Verwaltung**.
2. Beim ersten Start wird automatisch der Konfigurationsassistent für Remote-Administration gestartet. Details zu den einzelnen Schritte des Assistenten:
   a. Geben Sie im Fenster **Kennwortschutz** das Administratorkennwort ein oder ändern Sie es.
   b. Wählen Sie im Fenster **Netzwerk-Scan** ein Netzwerk für die Fernverwaltung.
   c. Wählen Sie im Fenster **Updatequelle** eine Methode für das Update der Antiviren-Datenbanken.
   d. Bestätigen Sie im Fenster **Übersicht** die ausgewählten Parameter.

   Bei späteren Starts ist die Eingabe des Administratorkennworts erforderlich.
3. Klicken Sie im folgenden Fenster **Verwaltung** auf das Statussymbol oder auf die Leiste, auf der sich das Symbol befindet.

   Die aktuellen Probleme werden im folgenden Fenster **Schutzstatus für Netzwerk** angezeigt.

- *Gehen Sie folgendermaßen vor, um eine Liste der auf einem Computer des lokalen Netzwerks vorliegenden Probleme anzuzeigen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im unteren Fensterbereich auf **Verwaltung**.
2. Beim ersten Start wird automatisch der Konfigurationsassistent für Remote-Administration gestartet. Details zu den einzelnen Schritte des Assistenten:
   a. Geben Sie im Fenster **Kennwortschutz** das Administratorkennwort ein oder ändern Sie es.
   b. Wählen Sie im Fenster **Netzwerk-Scan** ein Netzwerk für die Fernverwaltung.
   c. Wählen Sie im Fenster **Updatequelle** eine Methode für das Update der Antiviren-Datenbanken.
   d. Bestätigen Sie im Fenster **Übersicht** die ausgewählten Parameter.

   Bei späteren Starts ist die Eingabe des Administratorkennworts erforderlich.
3. Wählen Sie im oberen Bereich des folgenden Fensters **Verwaltung** den Computer aus, für den eine Problemliste angezeigt werden soll, und gehen Sie zum Abschnitt **Informationen**.
4. Wählen Sie im rechten Fensterbereich den Punkt **Liste der Probleme**.
5. Die aktuellen Probleme des ausgewählten Computers werden im folgenden Fenster **Schutzstatus** angezeigt.

WIE IHRE PERSÖNLICHEN DATEN VOR DIEBSTAHL GESCHÜTZT WERDEN.

Mit Kaspersky PURE können Sie Ihre persönlichen Daten vor Diebstahl schützen. Zu diesen zählen beispielsweise:

- Kennwörter, Benutzernamen und andere Anmeldedaten
- Konto- und Kreditkartennummern
- vertrauliche Dateien

Kaspersky PURE enthält Komponenten und Tools, mit denen Ihre persönlichen Daten vor Diebstahl geschützt werden können, wenn Angreifer Methoden wie Phishing und das Abfangen von Daten, die über die Tastatur eingegeben werden, einsetzen.

Für den Schutz vor Phishing ist Anti-Phishing verantwortlich, das zu den Komponenten Web-Anti-Virus, Anti-Spam und IM-Anti-Virus gehört.

Zum Schutz vor dem Abfangen von Daten, die über die Tastatur eingegeben werden, dienen die Virtuelle Tastatur und der Password Manager.

Die Datenverschlüsselung schützt Dateien vor unbefugtem Zugriff.

IN DIESEM ABSCHNITT

Schutz vor Phishing 70

Virtuelle Tastatur 71

Password Manager 71

Datenverschlüsselung 72

SCHUTZ VOR PHISHING

Phishing ist eine Art des Internetbetrugs, bei der Kreditkartennummern, PIN-Codes und andere persönliche Daten "geangelt" werden, um Geld zu stehlen.

Phishing ist häufig mit Online-Banking verbunden. Die Angreifer erstellen eine exakte Kopie der Homepage einer bestimmten Bank und schreiben die Kunden im Namen der Bank Briefe an. Den Kunden wird mitgeteilt, im Online-Banking-System seien aufgrund einer Störung oder Softwareaktualisierung die Benutzerdaten verloren gegangen und der Kunde solle die Daten auf der Bankseite bestätigen oder ändern. Folgt der Benutzer dem Link, der auf die Webseite der Angreifer führt, und gibt dort seine Daten ein, so fallen diese den Angreifern in die Hände.

Für den Schutz vor Phishing ist Anti-Phishing verantwortlich, das zu den Komponenten Web-Anti-Virus, Anti-Spam und IM-Anti-Virus gehört. Aktivieren Sie diese Komponenten, um einen effektiven Phishing-Schutz zu gewährleisten.

Gehen Sie folgendermaßen vor, um die Komponenten für den Phishing-Schutz zu aktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.

4. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Web-Anti-Virus aktivieren**.

5. Wiederholen Sie die Schritte 3 und 4 für die Komponenten **Anti-Spam** und **IM-Anti-Virus**.

   Es werden Komponenten aktiviert, zu denen auch Anti-Phishing gehört.

VIRTUELLE TASTATUR

Bei der Arbeit auf einem Computer ist es häufig erforderlich, persönliche Daten, Benutzername und Kennwort einzugeben. Beispiele sind die Anmeldung auf Internetseiten, der Besuch von Online-Shops usw.

In solchen Situationen besteht die Gefahr, dass persönliche Informationen mit Hilfe von Hardware-Hooks oder mit Keyloggern (Programme, die Tasteneingaben registrieren) abgefangen werden.

Die virtuelle Tastatur ermöglicht es, das Abfangen von über die Tastatur eingegebenen Daten zu verhindern.

Die virtuelle Tastatur kann Ihre persönlichen Daten nicht schützen, wenn eine Webseite gehackt wurde und die Eingabe solcher Daten fordert, weil die Informationen in diesem Fall dem Angreifer direkt in die Hände fallen.

Viele Spyware-Programme besitzen Funktionen zum Anlegen von Screenshots, die an Angreifer für Analyse und Sammeln von persönlichen Benutzerdaten automatisch übergeben werden. Die virtuelle Tastatur schützt vor Abfangen von eingegebenen persönlichen Daten durch Anlegen von Screenshots.

Die virtuelle Tastatur schützt persönliche Daten nur dann vor Diebstahlversuchen, wenn Sie mit den Internetbrowsern Microsoft Internet Explorer und Mozilla Firefox arbeiten.

➧ *Gehen Sie folgendermaßen vor, um die virtuelle Tastatur zu verwenden:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im unteren Fensterbereich auf **Virtuelle Tastatur**.

2. Geben Sie die erforderlichen Daten über die virtuelle Tastatur ein. Vergewissern Sie sich, dass die Daten im erforderlichen Feld eingegeben wurden. Die Funktionstasten (**Umschalt** , **Alt**, **Strg**) der virtuellen Tastatur verfügen über eine Einrastfunktion (wenn beispielsweise die **Umschalt**-Taste einmal angeklickt wurde, werden alle Zeichen groß geschrieben). Um die Einrastfunktion aufzuheben, klicken Sie erneut auf die Funktionstaste.

Die Sprache der virtuellen Tastatur lässt sich durch folgende Tastenkombination umschalten: **Strg** + Rechtsklick auf die **Umschalt**-Taste oder **Strg** + Rechtsklick auf **Alt**-Taste (von den Einstellungen abhängig).

PASSWORD MANAGER

Der Password Manager schützt Ihre persönlichen Daten (z.B. Benutzernamen, Kennwörter, Adressen, Telefon- und Kreditkartennummern).

Alle Informationen werden in verschlüsselter Form in einer Kennwort-Datenbank gespeichert, auf die der Zugriff nur mit einem Master-Kennwort möglich ist. Password Manager assoziiert Kennwörter und Benutzerkonten mit Programmen von Microsoft Windows oder mit Webseiten, für die sie verwendet werden. Nach dem Start einer Webseite oder eines Programms fügt Password Manager automatisch das Kennwort, den Benutzernamen und andere persönliche Daten ein. Somit ist es ausreichend, sich nur ein Kennwort zu merken und sich nicht alle Kennwörter einzuprägen.

➧ *Gehen Sie folgendermaßen vor, um für den Password Manager für das automatische Ausfüllen von Login-Formularen zu verwenden:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im unteren Fensterbereich auf **Password Manager**.

2. Beim ersten Start wird automatisch der Konfigurationsassistent für den Password Manager gestartet. Details zu den einzelnen Schritte des Assistenten:

a. Legen Sie im Fenster **Master-Kennwort** ein Master-Kennwort für den Schutz Ihrer Kennwort-Datenbank fest.

b. Wählen Sie im Fenster **Zugriffsverwaltung** eine Authentifizierungsmethode für den Zugriff auf Ihre Kennwort-Datenbank aus.

c. Legen Sie im Fenster **Zeitspanne bis zum Blockieren** fest, nach welcher Zeitspanne der Password Manager automatisch blockiert werden soll.

Bei späteren Starts ist die Eingabe des Master-Kennworts erforderlich.

3. Klicken Sie im folgenden Fenster auf **Kennwort hinzufügen**.

4. Wählen Sie im folgenden Assistentenfenster einen Typ für das Benutzerkonto aus (Benutzerkonto für das Internet, Benutzerkonto für ein Programm oder benutzerdefinierter Modus) und klicken Sie auf **Weiter**.

   - Wenn Sie ein Benutzerkonto für das Internet oder für ein Programm ausgewählt haben, geben Sie eine Webseite oder ein Programm an, für das dieses Benutzerkonto dienen soll, und klicken Sie auf **Weiter**.

   - Wenn Sie den erweiterten Modus ausgewählte haben, geben Sie auf der Registerkarte **Assoziation** einen Programmpfad / eine Webseite an und passen Sie die Verwendung des Benutzerkontos an.

5. Geben Sie im oberen Fensterbereich im Feld **Name** einen Namen für das neue Benutzerkonto ein oder ändern Sie den Namen.

6. Geben Sie auf der Registerkarte **Zugangsdaten** den Benutzernamen und das Kennwort an.

7. Passen Sie bei Bedarf auf der Registerkarte **Formular manuell ändern** die Parameter für das Ausfüllen von anderen Feldern auf einer Webseite an.

8. Geben Sie bei Bedarf auf der Registerkarte **Kommentar** eine Erläuterung für das Benutzerkonto an. Damit der Kommentar nach der Aktivierung des Benutzerkontos in einer Meldung erscheint, aktivieren Sie das Kontrollkästchen **Kommentare in Meldung anzeigen**.

9. Schließen Sie das Fenster mit **OK**.

10. Starten Sie das Programm / die Webseite, für das/die das Benutzerkonto angelegt wurde.

    Das Authentifizierungsformular wird auf Grundlage der Daten des Benutzerkontos automatisch ausgefüllt.

DATENVERSCHLÜSSELUNG

Um private Daten vor unbefugtem Zugriff zu schützen, wird empfohlen, diese in verschlüsselter Form in einem Spezialcontainer zu speichern.

Erstellen Sie einen Container, speichern Sie die Daten darin und verschlüsseln Sie anschließend die Daten. Danach ist für den Zugriff auf Daten, die sich in diesem Container befinden, die Eingabe des Kennworts erforderlich.

➧ *Gehen Sie folgendermaßen vor, um einen verschlüsselten Container anzulegen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Datenverschlüsselung**.

2. Klicken Sie im folgenden Fenster auf die die Schaltfläche **Container erstellen**.

3. Dadurch wird der Assistent für neue verschlüsselte Container gestartet. Details zu den einzelnen Schritte des Assistenten:

   a. Geben Sie im Fenster **Allgemeine Parameter** einen Namen, die Größe und ein Kennwort für den Container an.

   b. Legen Sie im Fenster **Pfad** den Ort der Containerdatei fest.

c. Wählen Sie einen Buchstaben für das virtuelle Laufwerk, legen Sie bei Bedarf zusätzliche Einstellungen fest und bestätigen Sie im Fenster **Übersicht**, dass ein Container mit den genannten Einstellungen angelegt werden soll.

Gehen Sie folgendermaßen vor, um Daten in einem Container zu speichern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Datenverschlüsselung**.
2. Wählen Sie im folgenden Fenster einen Container aus der Liste aus und klicken Sie auf **Öffnen**.

   Der Container wird im Fenster von Microsoft Windows Explorer geöffnet.
3. Speichern Sie die Daten, die verschlüsselt werden sollen, in dem Container.
4. Klicken Sie im Fenster **Datenverschlüsselung** auf **Daten verschlüsseln**.

Gehen Sie folgendermaßen vor, um Zugriff auf die Daten in einem Container zu erhalten:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Datenverschlüsselung**.
2. Wählen Sie im folgenden Fenster einen Container aus der Liste aus und klicken Sie auf **Daten entschlüsseln**.
3. Geben Sie im folgenden Fenster das Kennwort für den Zugriff auf den Container ein.
4. Klicken Sie im Fenster **Datenverschlüsselung** auf **Öffnen**.

WAS TUN, WENN SIE VERMUTEN, DASS EIN OBJEKT VON EINEM VIRUS INFIZIERT IST?

Wenn Sie den Verdacht haben, dass ein Objekt infiziert ist, sollten Sie es zuerst mit Hilfe von Kaspersky PURE untersuchen (s. Abschnitt "Untersuchung von Dateien, Ordnern, Laufwerken und anderen Objekten auf Viren" auf S. 66).

Wenn ein Objekt bei der Untersuchung vom Programm als virenfrei eingestuft wird, Sie aber vermuten, dass es infiziert ist, können Sie folgendermaßen vorgehen:

- Objekt in die *Quarantäne* verschieben. Objekte, die in die Quarantäne verschoben wurden, stellen keine Gefahr für Ihren Computer dar. Möglicherweise kann die Bedrohung eindeutig bestimmt und desinfiziert werden, nachdem die Datenbanken von Kaspersky PURE aktualisiert wurden.
- Objekt an das *Virenlabor* schicken. Die Experten des Virenlabors untersuchen das Objekt. Falls es tatsächlich infiziert ist, wird den Datenbanken eine Beschreibung des neuen Virus hinzugefügt. Die Datenbanken werden beim Update vom Programm aktualisiert (s. Abschnitt "Aktualisierung von Programmdatenbanken und -modulen" auf S. 65).

Ein Objekt kann auf zwei Arten in die Quarantäne verschoben werden:

- mit dem Link **In die Quarantäne verschieben** im Fenster **Schutzstatus**.
- mit Hilfe des Kontextmenüs für ein Objekt

Gehen Sie folgendermaßen vor, um vom Fenster Schutzstatus aus ein Objekt in die Quarantäne zu verschieben:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.
2. Klicken Sie im folgenden Fenster oben auf den Link **Quarantäne**, um das Fenster **Schutzstatus** zu öffnen.
3. Klicken Sie auf der Registerkarte **Erkannte Bedrohungen** auf den Link **In die Quarantäne verschieben**.
4. Wählen Sie im folgenden Fenster das Objekt, das in die Quarantäne verschoben werden soll.

- *Gehen Sie folgendermaßen vor, um ein Objekt mit Hilfe des Kontextmenüs in die Quarantäne zu verschieben:*

1. Öffnen Sie das Fenster von Microsoft Windows Explorer und gehen Sie in den Ordner mit dem Objekt, das in die Quarantäne verschoben werden soll.

Öffnen Sie durch Rechtsklick das Kontextmenü für das Objekt und wählen Sie den Punkt **In die Quarantäne verschieben**.

- *Gehen Sie folgendermaßen vor, um ein Objekt an das Virenlabor zu schicken:*

1. Gehen Sie auf die Seite, ie zum Senden einer Anfrage an das Virenlabor dient (http://support.kaspersky.ru/virlab/helpdesk.html?LANG=de).

2. Folgen Sie den Anweisungen, die auf dieser Seite gegeben werden, um eine Anfrage zu schicken.

WIE EIN OBJEKT WIEDERHERGESTELLT WIRD, DAS VOM PROGRAMM GELÖSCHT ODER DESINFIZIERT WURDE.

Kaspersky Lab warnt davor, gelöschte und desinfizierte Objekte wiederherzustellen, weil diese eine Gefahr für Ihren Computer darstellen können.

Wenn die Wiederherstellung eines gelöschten oder desinfizierten Objekts erforderlich ist, verwenden Sie dazu die Sicherungskopie, die vom Programm bei der Untersuchung des Objekts angelegt wurde.

- *Gehen Sie folgendermaßen vor, um ein Objekt wiederherzustellen, das vom Programm gelöscht oder desinfiziert wurde:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.

2. Klicken Sie im folgenden Fenster oben auf den Link **Quarantäne**, um das Fenster **Schutzstatus** zu öffnen.

3. Wählen Sie auf der Registerkarte **Erkannte Bedrohungen** in der Dropdown-Liste, die sich über der Bedrohungsliste befindet, das **Element Neutralisierte aus**.

   Die Registerkarte **Erkannte Bedrohungen** enthält eine Liste der desinfizierten und gelöschten Objekte. Die Objekte sind ihrem Status nach angeordnet. Klicken Sie links von der Überschrift einer Gruppe auf das Zeichen **+**, um eine Liste mit den Objekten einer Gruppe anzuzeigen.

4. Öffnen Sie durch Rechtsklick das Kontextmenü für das wiederherzustellende Objekt und wählen Sie im Menü den Punkt **Wiederherstellen**.

WAS TUN, WENN SIE VERMUTEN, DASS IHR COMPUTER INFIZIERT IST?

Wenn Sie vermuten, dass Ihr Computer infiziert ist, verwenden Sie den *Assistenten zur Systemwiederherstellung*, der die Spuren von schädlichen Objekten im System beseitigt. Die Kaspersky-Lab-Experten empfehlen außerdem, den Assistenten nach einer Desinfektion des Computers auszuführen, um sicherzustellen, dass alle aufgetretenen Bedrohungen und Beschädigungen beseitigt wurden.

Der Assistent prüft, ob im System Veränderungen vorliegen. Dazu zählen z.B. blockierter Zugriff auf die Netzwerkumgebung, veränderte Dateierweiterungen bekannter Formate, blockierte Systemsteuerung usw. Es gibt unterschiedliche Gründe für das Auftreten solcher Beschädigungen. Es kann sich um die Aktivität schädlicher Programme, inkorrekte Systemeinstellungen, Systemabstürze oder die Verwendung inkorrekt funktionierender Systemoptimierungsprogramme handeln.

Nach der Untersuchung analysiert der Assistent die gesammelten Informationen, um festzustellen, ob im System Beschädigungen vorliegen, die sofort behoben werden müssen. Aufgrund der Untersuchungsergebnisse wird eine Liste von Aktionen erstellt, die ausgeführt werden müssen, um die Beschädigungen zu beheben. Der Assistent ordnet die Aktionen nach der Priorität der gefundenen Probleme in Kategorien an.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**. Zum Abschluss des Assistenten dient die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf **Abbrechen** abgebrochen werden.

Gehen Sie folgendermaßen vor, den Assistenten zur Systemwiederherstellung zu starten:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im unteren Fensterbereich auf **Zusätzliche Funktionen**.
2. Klicken Sie im folgenden Fenster **Zusätzliche Funktionen** auf **Wiederherstellung nach Infektion**.

Details zu den einzelnen Schritte des Assistenten

Schritt 1. Systemwiederherstellung starten

Vergewissern Sie sich, dass im Assistentenfenster die Variante **Suche nach Problemen, die mit Malware-Aktivität zusammenhängen, durchführen** gewählt wurde, und klicken Sie auf **Weiter**.

Schritt 2. Nach Problemen suchen

Der Assistent sucht nach Problemen und möglichen Beschädigungen, die behoben werden müssen. Der Assistent geht nach Abschluss der Suche automatisch zum nächsten Schritt.

Schritt 3. Aktionen für die Problembehebung wählen

Alle Beschädigungen, die beim vorherigen Schritt gefunden wurden, werden ihrer Gefährlichkeit nach angeordnet. Für jede Gruppe von Beschädigungen schlagen die Kaspersky-Lab-Spezialisten eine Auswahl von Aktionen vor, deren Ausführung die Beschädigungen beheben kann. Die Aktionen sind in drei Gruppen unterteilt:

- *Ausdrücklich empfohlene Aktionen* können Beschädigungen beheben, die ein ernsthaftes Problem darstellen. Es wird empfohlen, alle Aktionen dieser Gruppe auszuführen.
- *Empfohlene Aktionen* dienen zum Beheben von Beschädigungen, die ein potentielles Risiko darstellen können. Es wird empfohlen, auch alle Aktionen dieser Gruppe auszuführen.
- *Zusätzliche Aktionen* dienen dazu, momentan ungefährliche Beschädigungen des Systems zu beheben, die die Computersicherheit in Zukunft bedrohen können.

Klicken Sie links vom Namen einer Gruppe auf das Zeichen **+**, um die Aktionen der Gruppe anzuzeigen.

Um eine bestimmte Aktion auszuführen, aktivieren Sie das Kontrollkästchen links vom Namen der Aktion. In der Grundeinstellung werden alle empfohlenen und ausdrücklich empfohlenen Aktionen ausgeführt. Soll eine bestimmte Aktion nicht ausgeführt werden, dann deaktivieren Sie das entsprechende Kontrollkästchen

Die standardmäßig aktivierten Kontrollkästchen sollten auf keinen Fall entfernt werden, weil dadurch die Sicherheit Ihres Computers bedroht wird.

Klicken Sie auf **Weiter**, nachdem Sie die Aktionen gewählt haben, die der Assistent ausführen soll.

Schritt 4. Probleme beheben

Der Assistent führt die Aktionen aus, die beim vorherigen Schritt festgelegt wurden. Die Problembehebung kann eine gewisse Zeit beanspruchen. Der Assistent geht nach Abschluss der Problembehebung automatisch zum nächsten Schritt.

Schritt 5. Assistent abschließen

Klicken Sie auf die Schaltfläche **Beenden**, um den Assistenten abzuschließen.

WIE SICHERUNGSKOPIEN IHRER DATEN ANGELEGT WERDEN

Die wichtigste Maßnahme, um wichtige Daten vor Verlust zu schützen, besteht in einer rechtzeitigen Datensicherung. Kaspersky PURE erlaubt es, automatisch eine regelmäßige Sicherung von ausgewählten Daten auszuführen. Dabei wird ein festgelegter Speicher verwendet und die Sicherung verläuft nach Zeitplan. Es kann auch eine einmalige Sicherung ausgeführt werden.

Zu Beginn der Arbeit muss auf dem ausgewählten Datenträger ein Backup-Speicher erstellt werden. In diesem Speicher werden Sicherungskopien für die erforderlichen Dateien angelegt. Anschließend können Sie die Backup-Aufgaben anpassen (Dateien auswählen, für die Sicherungskopien angelegt werden sollen, Zeitplan für den regelmäßigen automatischen Start und sonstige Sicherungsbedingungen festlegen).

- *Gehen Sie folgendermaßen vor, um einen Backup-Speicher anzulegen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Backup**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Backup-Speicher** und klicken Sie auf **Erstellen**.
3. Dadurch wird der Assistent für neue Backup-Speicher gestartet. Details zu den einzelnen Schritte des Assistenten:
   a. Wählen Sie auf der linken Seite des Fensters **Laufwerk** den Typ des Datenträgers, der als Speicher verwendet werden soll.

      Um die Daten besser zu schützen, wird empfohlen, die Backup-Speicher auf Wechseldatenträgern anzulegen.

   b. Legen Sie im Fenster **Schutz** ein Kennwort fest, um die Daten in diesem Speicher vor unerlaubtem Zugriff zu schützen (falls erforderlich).
   c. Beschränken Sie im Fenster **Dateiversionen** die Anzahl der Dateiversionen, die sich gleichzeitig im Speicher befinden dürfen, sowie die Speicherdauer für Sicherungskopien (falls erforderlich).
   d. Geben Sie im Fenster **Übersicht** einen Namen für den neuen Speicher an und bestätigen Sie, dass der Speicher mit diesen Parametern erstellt werden soll.

- *Gehen Sie folgendermaßen vor, um eine Sicherung auszuführen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Backup**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Backup** und klicken Sie auf **Erstellen**.
3. Dadurch wird der Assistent für neue Backup-Aufgaben gestartet. Details zu den einzelnen Schritte des Assistenten:
   a. Wählen Sie im Fenster **Inhalt** die Objekte, für die Sicherungskopien angefertigt werden sollen.
   b. Wählen Sie im Fenster **Speicher** den Speicher, in dem die Sicherungskopien abgelegt werden sollen.
   c. Legen Sie im Fenster **Zeitplan** die Startbedingungen für die Aufgabe fest.

      Wenn Sie eine einmalige Sicherung ausführen möchten, aktivieren Sie das Kontrollkästchen **Nach Zeitplan starten** nicht.

d. Geben Sie den Namen der neuen Aufgabe ein und klicken Sie im Fenster **Übersicht** auf **Beenden**.

Gehen Sie folgendermaßen vor, um Daten aus einer Sicherungskopie wiederherzustellen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Backup**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Daten wiederherstellen**.
3. Wählen Sie den Speicher, in dem sich die erforderlichen Sicherungskopien befinden, und klicken Sie auf **Daten wiederherstellen**.
4. Wählen Sie im oberen Bereich des Fensters **Daten wiederherstellen aus Speicher** aus der Dropdown-Liste ein Archiv aus (Zusammenstellung von Daten, die im Rahmen einer Aufgabe gespeichert wurden).
5. Wählen Sie die Dateien aus, die wiederhergestellt werden sollen. Aktivieren Sie dazu in der Liste die Kontrollkästchen der entsprechenden Dateien. Klicken Sie unter der Liste auf **Alle auswählen**, um alle Dateien auszuwählen. Klicken Sie im oberen Bereich des Fensters auf **Wiederherstellen**.
6. Geben Sie im folgenden Fenster **Wiederherstellung** an, wo wiederhergestellte Dateien gespeichert werden sollen, und legen Sie das Vorgehen bei einer Namensübereinstimmung fest. Klicken Sie auf **Wiederherstellen**.

   Die letzten Versionen der ausgewählten Dateien werden wiederhergestellt.

WIE DER ZUGRIFF AUF DIE EINSTELLUNGEN VON KASPERSKY PURE EINGESCHRÄNKT WIRD

Es kann sein, dass ein PC von mehreren Benutzern verwendet wird, deren Fertigkeiten im Umgang mit Computern völlig unterschiedlich sind. Der uneingeschränkte Zugriff der Benutzer auf Kaspersky PURE und dessen Einstellungen kann das Sicherheitsniveau des Computers stark beeinträchtigen.

Um den Zugriff auf das Programm zu beschränken, können Sie ein Kennwort festlegen und angeben, für welche Aktionen dieses abgefragt werden soll:

- Programmparameter ändern
- Backup verwalten
- Kindersicherung verwalten
- Netzwerksicherheit fernverwalten
- Programm beenden

Gehen Sie folgendermaßen vor, um den Zugriff auf Kaspersky PURE durch ein Kennwort zu schützen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Administratorkennwort** den Unterabschnitt **Allgemeine Einstellungen** aus.
4. Aktivieren Sie im rechten Fensterbereich im Block **Kennwortschutz** das Kontrollkästchen **Kennwortschutz aktivieren** und füllen Sie die Felder **Neues Kennwort** und **Kennwort bestätigen** aus.
5. Im Block **Gültigkeitsbereich des Kennworts** wird der Bereich festgelegt, für den die Zugriffsbeschränkung gelten soll. Beim Versuch eines beliebigen Benutzers, auf Ihrem Computer die von Ihnen ausgewählten Aktionen auszuführen, wird Kaspersky PURE nun immer das Kennwort abfragen.

Gehen Sie folgendermaßen vor, um das Kennwort für den Zugriff auf Kaspersky PURE zu ändern:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Administratorkennwort** den Unterabschnitt **Allgemeine Einstellungen** aus.
4. Füllen Sie im rechten Fensterbereich im Block **Kennwortschutz** die Felder **Altes Kennwort**, **Neues Kennwort** und **Kennwort bestätigen** aus.

WIE DIE VERWENDUNG DES COMPUTERS UND INTERNETS FÜR VERSCHIEDENE BENUTZER EINGESCHRÄNKT WIRD

Unmittelbar nach der Installation von Kaspersky PURE bestehen keinerlei Beschränkungen für die Computerbenutzer. Um Kinder und Jugendliche vor Gefahren zu schützen, die bei der Arbeit am Computer bestehen, ist es erforderlich, die Kindersicherung für alle Computerbenutzer rechtzeitig anzupassen.

Wenn Sie den Kennwortschutz bei der Programminstallation nicht aktiviert haben (s. Abschnitt "Schritt 16. Kontrolle des Zugriffs auf das Programm" auf S. 36), wird empfohlen, beim ersten Start der Kindersicherung ein Kennwort festzulegen, damit die Kontrolleinstellungen nicht von Unbefugten geändert werden können. Anschließend können Sie die Kindersicherung aktivieren und Beschränkungen anpassen, die die Verwendung des Computers und des Internets für alle Benutzerkonten des Computers regulieren.

Gehen Sie folgendermaßen vor, um die Kindersicherung für ein Benutzerkonto anzupassen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Kindersicherung**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Benutzer**.
3. Klicken Sie auf der rechten Fensterseite auf **Aktivieren**.
4. Wählen Sie aus der Benutzerkontenliste das Benutzerkonto aus, für das die Kontrollparameter angepasst werden sollen, und klicken Sie auf **Anpassen**.
5. Wählen Sie im linken Bereich des folgenden Fensters einen Beschränkungstyp aus und passen Sie rechts die Kontrolleinstellungen an.

WIE EINE NOTFALL-CD ERSTELLT UND VERWENDET WIRD.

Es wird empfohlen, Kaspersky PURE auf dem Computer zu installieren und anzupassen, und den Computer dann zu untersuchen, um sicherzustellen, dass er virenfrei ist. Anschließend können Sie eine Notfall-CD erstellen. Die Notfall-CD kann später verwendet werden, um den infizierten Computer zu untersuchen und zu desinfizieren, wenn eine Desinfektion mit anderen Mitteln (z.B. Antiviren-Programme) fehlschlägt.

IN DIESEM ABSCHNITT

Notfall-CD erstellen 79

Hochfahren eines Computers mit Hilfe der Notfall-CD 80

NOTFALL-CD ERSTELLEN

Das Anlegen einer Notfall-CD umfasst das Erstellen eines Disk-Abbild (iso-Datei) mit den aktuellen Programm-Datenbanken und Konfigurationsdateien.

Ein Original des Disk-Abbilds, auf dessen Basis eine neue Datei erstellt wird, kann von einem Kaspersky-Lab-Server heruntergeladen oder aus einer lokalen Quelle kopiert werden.

Die Notfall-CD wird mit Hilfe des *Assistenten zum Erstellen einer Notfall-CD* erstellt. Die vom Assistenten angelegte Abbild-Datei rescuecd.iso wird auf der Festplatte Ihres Computers gespeichert:

- im Betriebssystem Microsoft Windows XP – im Ordner Dokumente und Einstellungen\All Users\Application Data\Kaspersky Lab\AVP9\Data\Rdisk\.
- in Betriebssystemen Microsoft Windows Vista und Microsoft Windows 7 – im Ordner ProgramData\Kaspersky Lab\AVP9\Data\Rdisk\.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**. Zum Abschluss des Assistenten dient die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf **Abbrechen** abgebrochen werden.

Gehen Sie folgendermaßen vor, um Assistenten zum Erstellen einer Notfall-CD zu starten:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im unteren Fensterbereich auf **Zusätzliche Funktionen**.
2. Klicken Sie im folgenden Fenster **Zusätzliche Funktionen** auf **Notfall-CD**.

Details zu den einzelnen Schritte des Assistenten

Schritt 1. Quelle für Disk-Abbild auswählen

Auf dieser Etappe muss aus folgenden Varianten eine Quelle für die Abbild-Datei gewählt werden:

- Wählen Sie die Variante **Abbild von lokaler Festplatte oder Netzlaufwerk kopieren**, wenn Sie über eine fertige Notfall-CD verfügen oder auf Ihrem Computer bzw. in einer Ressource des lokalen Netzwerks ein dafür vorbereitetes Abbild bereitliegt.
- Wählen Sie die Variante **Abbild von Kaspersky-Lab-Server herunterladen**, wenn Sie nicht über eine fertige Abbild-Datei verfügen und diese von einem Kaspersky-Lab-Server herunterladen möchten (die Dateigröße beträgt ungefähr 175 MB).

Schritt 2. Disk-Abbild kopieren (herunterladen)

Wenn Sie beim vorherigen Schritt die Variante zum Kopieren des Abbild aus einer lokalen Quelle gewählt haben (**Abbild von lokaler Festplatte oder Netzlaufwerk kopieren**), geben Sie bei diesem Schritt den entsprechenden Pfad an. Klicken Sie dazu auf die Schaltfläche **Durchsuchen**. Nachdem Sie den Pfad zur Datei angegeben haben, klicken Sie auf **Weiter**. Im Assistentenfenster wird angezeigt, wie das Kopieren des Disk-Abbilds verläuft.

Wenn Sie die Variante **Abbild von Kaspersky-Lab-Server herunterladen**, gewählt haben, wird sofort angezeigt, wie das Kopieren des Disk-Abbilds verläuft.

Nach Abschluss des Kopiervorgangs oder des Ladens des Disk-Abbilds wechselt der Assistent automatisch zum nächsten Schritt.

Schritt 3. Abbild-Datei aktualisieren

Der Vorgang zur Aktualisierung der Abbild-Datei umfasst:

- Update der Antiviren-Datenbanken.

- Aktualisierung der Konfigurationsdateien.

Die Konfigurationsdateien bestimmen die Möglichkeit zum Hochfahren des Computers von einer CD / DVD, die mit Hilfe eines Notfall-CD-Abbilds gebrannt wurde, das wiederum unter Verwendung des Assistenten erstellt wurde.

Für die Aktualisierung der Antiviren-Datenbanken werden die beim letzten Update von Kaspersky PURE heruntergeladenen Datenbanken verwendet. Wenn die Datenbanken veraltet sind, wird empfohlen, die Updateaufgabe auszuführen und den Notfall-CD-Assistenten erneut zu starten.

Klicken Sie auf die Schaltfläche **Weiter**, um die Aktualisierung der Datei zu starten. Im Assistentenfenster wird angezeigt, wie die Aktualisierung verläuft.

Schritt 4. Assistent abschließen

Klicken Sie auf **Beenden**, um die Arbeit des Assistenten abzuschließen Die erstellte iso-Datei kann auf einer CD / DVD-ROM gespeichert werden und später zum Booten des Computers verwendet werden.

HOCHFAHREN EINES COMPUTERS MIT HILFE DER NOTFALL-CD

Wenn sich das Betriebssystem aufgrund eines Virenangriffs nicht mehr hochfahren lässt, können Sie die Notfall-CD einsetzen.

Um das Betriebssystem zu booten ist eine CD/DVD-ROM mit der darauf gespeicherten Abbild-Datei (.iso) der Boot-Disk erforderlich.

Gehen Sie folgendermaßen vor, um den Computer von einer Notfall-CD zu booten:

1. Wählen Sie in den BIOS-Einstellungen das Booten von CD / DVD-ROM (weitere Informationen können der Dokumentation zum Motherboard Ihres Computers entnommen werden).
2. Legen Sie die CD / DVD-ROM, auf die das Disk-Abbild gebrannt wurde, in das CD / DVD-Laufwerk des infizierten Computers ein.
3. Starten Sie den Computer neu.

Ausführliche Informationen über die Verwendung der Notfall-CD bietet das Benutzerhandbuch zu Kaspersky Rescue Disk.

WIE MIT EINER GROßEN ANZAHL VON SPAM-MAILS VERFAHREN WIRD?

Wenn Sie viel Spam erhalten, aktivieren Sie die Komponente Anti-Spam, wählen Sie die empfohlene Sicherheitsstufe und trainieren Sie die Komponente dann mit dem *Trainingsassistenten*. Für die korrekte Spam-Erkennung ist es erforderlich, ein Training mit mindestens 50 Mustern erwünschter Mails und 50 Spam-Mustern vorzunehmen.

Gehen Sie folgendermaßen vor, um Anti-Spam zu aktivieren und die empfohlene Sicherheitsstufe zu wählen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
4. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Anti-Spam aktivieren**.
5. Im Block **Sicherheitsstufe** ist standardmäßig die Sicherheitsstufe **Empfohlen** eingestellt.

Sollte die Sicherheitsstufe **Niedrig** oder **Benutzerdefiniert** gewählt sein, so klicken Sie auf **Standard**. Die Sicherheitsstufe erhält automatisch den Wert **Empfohlen**.

Gehen Sie folgendermaßen vor, um Anti-Spam mit Hilfe des Trainingsassistenten zu trainieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
4. Klicken Sie auf der rechten Fensterseite im Block **Anti-Spam-Training** auf **Trainieren**.

   Das Fenster des Trainingsassistenten wird geöffnet.

Details zu den einzelnen Schritte des Assistenten

Schritt 1. Assistent starten

Klicken Sie auf **Weiter**, um mit dem Training zu beginnen.

Schritt 2. Ordner auswählen, die nützliche E-Mails enthalten

Auf dieser Etappe können Sie die Ordner wählen, die erwünschte E-Mails enthalten. Es dürfen nur Ordner gewählt werden, über deren Inhalt vollständige Sicherheit besteht.

Nur die Ordner von Benutzerkonten für Microsoft Office Outlook und Microsoft Outlook Express (Windows Mail) stehen zur Auswahl.

Schritt 3. Ordner wählen, die unerwünschte E-Mails enthalten

Auf dieser Etappe können Sie die Ordner wählen, die unerwünschte E-Mails (Spam) enthalten. Sollten in Ihrem Mailprogramm keine entsprechenden Ordner vorhanden sein, dann überspringen Sie diesen Schritt.

Nur die Ordner von Benutzerkonten für Microsoft Office Outlook und Microsoft Outlook Express (Windows Mail) stehen zur Auswahl.

Schritt 4. Anti-Spam-Training

Bei diesem Schritt findet das automatische Training von Anti-Spam statt. Dazu dienen die Ordner, die bei den vorhergehenden Schritten ausgewählt wurden. Die Anti-Spam-Datenbank wird durch die E-Mails aus diesen Ordnern ergänzt. Die Absender von erwünschten E-Mails werden automatisch in die Liste der erlaubten Absender aufgenommen.

Schritt 5. Trainingsergebnisse speichern

Auf dieser Etappe des Assistenten werden die Trainingsergebnisse auf eine der folgenden Arten gespeichert:

- Trainingsergebnisse zur bestehenden Anti-Spam-Datenbank hinzufügen (Variante **Anti-Spam-Datenbank durch Trainingsergebnisse ergänzen**).
- Bestehende Datenbank durch die neu erstellte Datenbank ersetzen (Variante **Neue Anti-Spam-Datenbank erstellen**).

Klicken Sie auf die Schaltfläche **Beenden**, um den Assistenten abzuschließen.

WIE EIN BERICHT ÜBER DEN COMPUTERSCHUTZ GEÖFFNET WIRD

Kaspersky PURE führt Berichte über die Arbeit der einzelnen Schutzkomponenten. Im Bericht können Sie beispielsweise feststellen, wie viele schädliche Objekte (z.B. Viren, trojanische Programme) das Programm in einem bestimmten Zeitraum gefunden und neutralisiert hat, wie oft das Programm in diesem Zeitraum aktualisiert wurde, wie viele Spam-Mails gefunden wurden, u.a.

Gehen Sie folgendermaßen vor, um einen Bericht über die Programmarbeit anzuzeigen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.

   Das Fenster **Computersicherheit** wird geöffnet.

2. Gehen Sie mit Hilfe des Links **Bericht** in das Berichtsfenster von Kaspersky PURE.

   Im folgenden Fenster werden auf der Registerkarte **Bericht** die Programmberichte in Form von Diagrammen dargestellt.

3. Klicken Sie im unteren Bereich der Registerkarte **Bericht** auf **Detaillierter Bericht**, um einen ausführlichen Bericht über die Arbeit des Programms zu öffnen (z.B. über die Arbeit der einzelnen Programmkomponenten).

   Das Fenster **Detaillierter Bericht** wird geöffnet. Hier werden die Daten in Tabellenform dargestellt. Die Berichtseinträge können auf unterschiedliche Weise angeordnet werden.

WIE DIE STANDARDEINSTELLUNGEN DES PROGRAMMS WIEDERHERGESTELLT WERDEN

Sie können jederzeit zu den empfohlenen Einstellungen für Kaspersky PURE zurückkehren. Diese gelten als optimal und werden von Kaspersky Lab empfohlen. Die Wiederherstellung der Einstellungen erfolgt mit Hilfe des Konfigurationsassistenten des Programms.

Im folgenden Fenster können Sie angeben, welche Parameter bei der Wiederherstellung der empfohlenen Sicherheitsstufe beibehalten werden sollen und für welche Komponenten diese gelten sollen.

Die Liste enthält die Komponenten von Kaspersky PURE, deren Einstellungen vom Benutzer verändert oder von Kaspersky PURE beim Training der Komponenten Firewall und Anti-Spam gesammelt wurden. Wenn für eine bestimmte Komponente bei der Arbeit unikale Parameter festgelegt wurden, werden diese ebenfalls in der Liste angegeben.

Als unikale Parameter gelten: Weiße und Schwarze Listen mit Phrasen und Adressen für die Komponente Anti-Spam, Listen mit vertrauenswürdigen Internetadressen und Telefonnummern von Internetprovidern, die von den Komponenten Web-Anti-Virus und Anti-Spy verwendet werden, für den Schutz geltende Ausnahmeregeln, Filterregeln für Pakete und Programme für die Komponente Firewall.

Diese Listen werden bei der Arbeit von Kaspersky PURE erstellt. Dabei werden individuelle Aufgaben und Sicherheitsanforderungen berücksichtigt. Das Erstellen der Listen ist sehr zeitaufwändig. Deshalb wird empfohlen, sie beim Wiederherstellen der ursprünglichen Programmeinstellungen zu speichern.

Nach dem Abschluss des Assistenten wird für alle Schutzkomponenten die Sicherheitsstufe **Empfohlen** eingestellt, wobei die von Ihnen zum Speichern gewählten Parameter berücksichtigt werden. Zusätzlich werden die Einstellungen übernommen, die Sie während der Arbeit des Assistenten vorgenommen haben.

Gehen Sie folgendermaßen vor, um die Schutzeinstellungen wiederherzustellen:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie auf der linken Fensterseite im Abschnitt **Allgemeine Einstellungen** den Abschnitt **Allgemein**.

4. Klicken Sie auf der rechten Fensterseite auf **Wiederherstellen**.

5. Klicken Sie im folgenden Fenster **Weiter**. Dadurch wird der Konfigurationsassistent gestartet. Folgen Sie den Anweisungen.

WIE DIE PROGRAMMEINSTELLUNGEN AUF EINEN ANDEREN COMPUTER ÜBERTRAGEN WERDEN

Sie können Ihre Programmeinstellungen für ein anderes Exemplar von Kaspersky PURE übernehmen, das auf einem anderen Computer installiert ist. Auf diese Weise sind die Einstellungen des Programms auf beiden Computern identisch. Diese Option kann beispielsweise von Nutzen sein, wenn Sie Kaspersky PURE auf Ihrem PC zuhause und im Büro installiert haben.

Die Programmeinstellungen werden in einer speziellen Konfigurationsdatei gespeichert, die Sie von Computer zu Computer übertragen können. Dabei gilt folgendes Vorgehen:

1. *Exportieren* Sie die Einstellungen, d.h. die Programmeinstellungen werden in eine Konfigurationsdatei kopiert.

2. Übertragen Sie die gespeicherte Datei auf einen anderen Computer (z.B. per E-Mail oder mit einem Wechseldatenträger).

3. *Importieren* Sie die Einstellungen, d.h. die Einstellungen werden aus einer Konfigurationsdatei in ein Programm übernommen, das auf einem anderen Computer installiert ist.

Gehen Sie folgendermaßen vor, um die aktuellen Einstellungen von Kaspersky PURE zu exportieren:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie auf der linken Fensterseite im Abschnitt **Allgemeine Einstellungen** den Abschnitt **Allgemein**.

4. Klicken Sie auf der rechten Fensterseite auf **Speichern**.

5. Geben Sie im folgenden Fenster einen Namen für die Konfigurationsdatei an und wählen Sie einen Speicherort dafür.

Gehen Sie folgendermaßen vor, um die Funktionsparameter aus einer Konfigurationsdatei zu importieren:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie auf der linken Fensterseite im Abschnitt **Allgemeine Einstellungen** den Abschnitt **Allgemein**.

4. Klicken Sie auf der rechten Fensterseite auf **Laden**.

5. Wählen Sie im folgenden Fenster eine Datei, aus der Sie die Einstellungen für Kaspersky PURE importieren möchten.

ERWEITERTE PROGRAMMEINSTELLUNGEN

Dieser Abschnitt informiert ausführlich über die einzelnen Komponenten und beschreibt den jeweiligen Funktionsalgorithmus und die Einstellungen.

IN DIESEM ABSCHNITT

Computersicherheit 85

Backup 171

Kindersicherung 178

Datenverschlüsselung 187

Verwaltung 191

Password Manager 195

Leistung und Kompatibilität mit anderen Programmen 226

Selbstschutz für Kaspersky PURE 229

Aussehen des Programms 230

Zusätzliche Funktionen 233

Berichte 239

Meldungen 244

Teilnahme an Kaspersky Security Network 245

COMPUTERSICHERHEIT

Die Komponenten der Computersicherheit schützen Ihren Computer vor unterschiedlichen Bedrohungen, untersuchen Systemobjekte auf Viren und Schwachstellen, und aktualisieren regelmäßig die Datenbanken und Programm-Module von Kaspersky PURE.

IN DIESEM ABSCHNITT

Untersuchung des Computers 85

Update 93

Datei-Anti-Virus 99

Mail-Anti-Virus 106

Web-Anti-Virus 111

IM-Anti-Virus 117

Anti-Spam 119

Anti-Banner 136

Programmkontrolle 138

Proaktiver Schutz 147

Netzwerkschutz 149

Vertrauenswürdige Zone 161

Sichere Umgebung für die Ausführung von Programmen 164

Quarantäne und Backup 168

UNTERSUCHUNG DES COMPUTERS

Die Untersuchung des Computers auf Viren und Schwachstellen ist eine der wichtigsten Funktionen für die Sicherheit des Rechners. Es ist erforderlich, Ihren Computer regelmäßig auf Viren zu scannen, um die Möglichkeit der Ausbreitung schädlicher Programme auszuschließen, die nicht von den Schutzkomponenten erkannt wurden, weil beispielsweise eine zu niedrige Schutzstufe eingestellt war.

Die Aufgabe zur Schwachstellensuche umfasst eine Sicherheitsdiagnose des Betriebssystems und eine Software-Analyse zum Erkennen von Sicherheitslücken, die Angreifern zur Verbreitung schädlicher Objekte und zum Zugriff auf persönliche Daten dienen können.

Die folgenden Abschnitte informieren ausführlich über Besonderheiten und Konfiguration von Untersuchungsaufgaben sowie über Sicherheitsstufen, Methoden und Technologien für die Untersuchung.

IN DIESEM ABSCHNITT

Virensuche 86

Suche nach Schwachstellen 93

VIRENSUCHE

Kaspersky PURE verfügt über folgende Aufgaben zur Virensuche:

- **Untersuchung von Objekten**. Es werden die vom Benutzer festlegten Objekte untersucht. Es kann ein beliebiges Objekt des Dateisystems auf dem Computer untersucht werden. Im Rahmen dieser Aufgabe können Sie die Parameter anpassen, die für die Untersuchung von Wechseldatenträgern gelten.

- **Vollständige Untersuchung**. Ausführliche Untersuchung des Systems. Standardmäßig werden folgende Objekte untersucht: Systemspeicher, Objekte, die beim Systemstart geladen werden, Systemwiederherstellung, Mail-Datenbanken, Festplatten, Wechseldatenträger und Netzlaufwerke.

- **Schnelle Untersuchung**. Es werden die Objekte untersucht, die beim Hochfahren des Betriebssystems gestartet werden.

Es wird davor gewarnt, die Liste der Untersuchungsobjekte für die Aufgaben zur vollständigen und schnellen Untersuchung zu ändern.

Jede Untersuchungsaufgabe wird in einem bestimmten Bereich ausgeführt und kann nach einem festgelegten Zeitplan gestartet werden. Außerdem wird jede Untersuchungsaufgabe durch eine Sicherheitsstufe charakterisiert (Auswahl von Einstellungen, die das Verhältnis von Leistung und Sicherheit beeinflussen). Standardmäßig ist immer der Modus zur Untersuchung mit Hilfe der Einträge der Programm-Datenbanken aktiviert. Außerdem können Sie verschiedene Methoden und Technologien zur Untersuchungs einsetzen s. S. 90).

Nach dem Start einer Untersuchungsaufgabe wird der Vorgang im Abschnitt **Untersuchung** des Fensters **Computersicherheit** im Feld unter dem Namen der laufenden Aufgabe angezeigt.

Beim Fund einer Bedrohung weist Kaspersky PURE dem gefundenen Objekt eine der folgenden Statusvarianten zu:

- Status eines der schädlichen Programme (beispielsweise *Virus*, *trojanisches Programm*).

- Status *möglicherweise infiziert* (verdächtig) wenn sich aufgrund der Untersuchung nicht eindeutig feststellen lässt, ob das Objekt infiziert ist oder nicht. Möglicherweise enthält die Datei eine virentypische Codefolge oder den modifizierten Code eines bekannten Virus.

Anschließend zeigt das Programm eine Meldung (s. S. 244) über die gefundene Bedrohung an und führt die festgelegte Aktion aus. Sie können die Aktion beim Fund einer Bedrohung ändern.

Wenn Sie im automatischen Modus (s. Abschnitt "Interaktiven Schutzmodus verwenden" auf S. 61), wendet Kaspersky PURE beim Fund gefährlicher Objekte automatisch die von Kaspersky Lab empfohlene Aktion an. Für schädliche Objekte ist dies die Aktion **Desinfizieren. Löschen, wenn Desinfektion nicht möglich**, für verdächtige – **In die Quarantäne verschieben**. Wenn Sie im interaktiven Modus arbeiten (s. Abschnitt "Interaktiven Schutzmodus verwenden" auf S. 61), zeigt das Programm beim Fund gefährlicher Objekte auf dem Bildschirm eine Meldung an, in der Sie eine Aktion auswählen können.

Bevor ein infiziertes Objekt desinfiziert oder gelöscht wird, legt Kaspersky PURE eine Sicherungskopie des Objekts an. Dadurch wird erlaubt, das Objekt bei Bedarf wiederherzustellen oder später zu desinfizieren. Verdächtige (möglicherweise infizierte) Objekte werden in die Quarantäne verschoben. Sie können eine automatische Untersuchung der Quarantänedateien nach jedem Update festlegen.

Informationen über die Untersuchungsergebnisse und über alle Ereignisse, die bei der Aufgabenausführung auftreten, werden im Bericht von Kaspersky PURE protokolliert.

IN DIESEM ABSCHNITT

Sicherheitsstufe ändern und wiederherstellen 87

Zeitplan für den Untersuchungsstart erstellen 88

Liste der Untersuchungsobjekte erstellen 88

Untersuchungsmethode auswählen 89

Untersuchungstechnologien wählen 90

Aktion beim Fund einer Bedrohung ändern 90

Untersuchungsstart mit den Rechten eines anderen Benutzers 90

Typ der zu untersuchenden Objekte ändern 90

Untersuchung von zusammengesetzten Dateien 91

Untersuchung optimieren 92

Wechseldatenträger beim Anschließen untersuchen 92

Verknüpfung für den Aufgabenstart erstellen 93

SICHERHEITSSTUFE ÄNDERN UND WIEDERHERSTELLEN

Sie können eine vordefinierte Sicherheitsstufe auswählen, die Ihren Anforderungen entspricht, oder die Untersuchungseinstellungen entsprechend anpassen.

Während Sie eine Untersuchungsaufgabe anpassen, können Sie jederzeit zu den empfohlenen Einstellungen zurückkehren. Diese gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und sind in der Sicherheitsstufe **Empfohlen** zusammengefasst.

Gehen Sie folgendermaßen vor, um die festgelegte Sicherheitsstufe zu ändern:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung des Computers** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Schnelle Untersuchung** oder **Untersuchung von Objekten**).
4. Stellen Sie für die gewählte Aufgabe im Block **Sicherheitsstufe** die erforderliche Sicherheitsstufe ein oder klicken Sie auf **Einstellungen**, um die Untersuchungseinstellungen manuell anzupassen.

Wenn manuelle Änderungen erfolgen, ändert sich der Name der Sicherheitsstufe in **Benutzerdefiniert**.

Gehen Sie folgendermaßen vor, um die empfohlenen Untersuchungseinstellungen wiederherzustellen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung des Computers** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Schnelle Untersuchung** oder **Untersuchung von Objekten**).
4. Klicken Sie für die ausgewählte Aufgabe im Block **Sicherheitsstufe** auf **Standard**.

ZEITPLAN FÜR DEN UNTERSUCHUNGSSTART ERSTELLEN

Es kann ein Zeitplan für den automatischen Start einer Untersuchungsaufgabe angelegt werden: In diesem werden eine Frequenz für den Aufgabenstart, ein Startzeitpunkt (falls erforderlich) sowie zusätzliche Parameter festgelegt.

Wenn der Start aus irgendeinem Grund nicht möglich war (wenn beispielsweise der Computer im betreffenden Moment ausgeschaltet war), können Sie festlegen, dass der Start einer übersprungenen Aufgabe automatisch zum nächstmöglichen Zeitpunkt erfolgt. Außerdem lässt sich festlegen, dass eine Untersuchung automatisch angehalten wird, wenn der Bildschirmschoner inaktiv oder der Computer nicht entsperrt ist. Diese Option erlaubt es, den Start einer Aufgabe zurückzustellen, bis der Benutzer seine Arbeit auf dem Computer beendet hat. Dadurch wird verhindert, dass eine Untersuchungsaufgabe Computerressourcen verbraucht, während diese für andere Aufgaben benötigt werden.

- *Gehen Sie folgendermaßen vor, um den Startzeitplan einer Untersuchungsaufgabe anzupassen:*

  1. Öffnen Sie das Programmhauptfenster.
  2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
  3. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung des Computers** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten** oder **Schwachstellensuche**).
  4. Klicken Sie für die ausgewählte Aufgabe im Block **Startmodus** auf **Einstellungen**.
  5. Wählen Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Zeitplan** die Option **Nach Zeitplan** aus und konfigurieren Sie den Startmodus für die Untersuchung.

- *Gehen Sie folgendermaßen vor, um den automatischen Start einer übersprungenen Aufgabe anzupassen:*

  1. Öffnen Sie das Programmhauptfenster das Programmhauptfenster.
  2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
  3. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung des Computers** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten** oder **Schwachstellensuche**).
  4. Klicken Sie für die ausgewählte Aufgabe im Block **Startmodus** auf **Einstellungen**.
  5. Wählen Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Zeitplan** die Option **Nach Zeitplan** aus und aktivieren Sie das Kontrollkästchen **Übersprungene Aufgaben starten**.

- *Gehen Sie folgendermaßen vor, damit die Untersuchung erst gestartet wird, nachdem der Benutzer seine Arbeit beendet hat:*

  1. Öffnen Sie das Programmhauptfenster.
  2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
  3. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung des Computers** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten** oder **Schwachstellensuche**).
  4. Klicken Sie für die ausgewählte Aufgabe im Block **Startmodus** auf **Einstellungen**.
  5. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Zeitplan** die Option **Nach Zeitplan** und aktivieren Sie das Kontrollkästchen **Geplante Untersuchung anhalten, wenn Bildschirmschoner inaktiv und Computer nicht blockiert ist**.

LISTE DER UNTERSUCHUNGSOBJEKTE ERSTELLEN

Standardmäßig entspricht jeder Aufgabe zur Virensuche eine eigene Liste von Objekten. Zu diesen Objekten können sowohl Objekte des Computerdateisystems (z.B. logische Laufwerke, **Mail-Datenbanken**), als auch Objekte anderer Typen (z.B. Netzlaufwerke) gehören. Diese Liste kann geändert werden.

Wenn der Untersuchungsbereich leer ist oder kein Objekt des Untersuchungsbereichs angekreuzt wurde, kann die Untersuchungsaufgabe nicht gestartet werden!

- *Gehen Sie folgendermaßen vor, um für eine Untersuchungsaufgabe eine Liste der Untersuchungsobjekte zu erstellen:*

  1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.

     Das Fenster **Computersicherheit** wird geöffnet.

  2. Wählen Sie auf der linken Fensterseite den Abschnitt **Untersuchung**.

  3. Klicken Sie im rechten Fensterbereich auf den Link **Hinzufügen**, um die Liste der Untersuchungsobjekte zu öffnen.

  4. Wählen Sie im folgenden Fenster **Untersuchungsobjekt wählen** ein Objekt und klicken Sie auf **Hinzufügen**. Nachdem alle erforderlichen Objekte hinzugefügt wurden, klicken Sie auf **OK**. Um bestimmte Objekte aus der Untersuchungsliste auszuschließen, deaktivieren Sie das entsprechende Kontrollkästchen.

- *Gehen Sie folgendermaßen vor, um für die Aufgaben zur schnellen Untersuchung, zur vollständigen Untersuchung oder zur Schwachstellensuche eine Liste mit Untersuchungsobjekten zu erstellen:*

  1. Öffnen Sie das Programmhauptfenster.

  2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

  3. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung des Computers** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Schnelle Untersuchung** oder **Schwachstellensuche**).

  4. Klicken Sie für die ausgewählte Aufgabe im Block **Untersuchungsobjekte** auf **Einstellungen**.

  5. Erstellen Sie im folgenden Fenster Untersuchungsobjekte mit Hilfe der Links **Hinzufügen**, **Ändern** und **Löschen** eine **Liste**. Um bestimmte Objekte aus der Untersuchungsliste auszuschließen, deaktivieren Sie das entsprechende Kontrollkästchen.

     Objekte, die sich standardmäßig in der Liste befinden, können nicht geändert oder gelöscht werden.

UNTERSUCHUNGSMETHODE AUSWÄHLEN

Bei einer Virenuntersuchung des Computers wird immer die Methode *Signaturanalyse* verwendet, bei der Kaspersky PURE ein gefundenes Objekt mit den Einträgen in den Datenbanken vergleicht.

Um die Effektivität der Suche zu steigern, stehen zusätzliche Untersuchungsmethoden zur Verfügung: *heuristische Analyse* (Analyse der Aktivität, die ein Objekt im System zeigt) und *Rootkit-Suche* (Utilities, die schädliche Programme im Betriebssystem verstecken).

- *Gehen Sie folgendermaßen vor, um die erforderlichen Untersuchungsmethoden zu verwenden:*

  1. Öffnen Sie das Programmhauptfenster.

  2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

  3. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung des Computers** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Schnelle Untersuchung** oder **Untersuchung von Objekten**).

  4. Klicken Sie für die ausgewählte Aufgabe im Block **Startmodus** auf **Einstellungen**.

  5. Wählen Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Untersuchungsmethoden** die erforderlichen Einstellungswerte aus.

UNTERSUCHUNGSTECHNOLOGIEN WÄHLEN

Neben den Untersuchungsmethoden können Sie spezielle Technologien einsetzen, mit denen das Untersuchungstempo gesteigert werden kann. Dabei werden Dateien ausgeschlossen, die seit dem letzten Scan nicht verändert wurden.

Gehen Sie folgendermaßen vor, um die Technologien zur Objektuntersuchung zu aktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung des Computers** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Schnelle Untersuchung** oder **Untersuchung von Objekten**).
4. Klicken Sie für die ausgewählte Aufgabe im Block **Startmodus** auf **Einstellungen**.
5. Wählen Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Untersuchungstechnologien** den erforderlichen Einstellungswert aus.

AKTION BEIM FUND EINER BEDROHUNG ÄNDERN

Beim Fund infizierter oder möglicherweise infizierter Objekte führt das Programm eine festgelegte Aktion aus.

Gehen Sie folgendermaßen vor, um die Aktion für gefundene Objekte zu ändern:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung des Computers** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Schnelle Untersuchung** oder **Untersuchung von Objekten**).
4. Geben Sie für die ausgewählte Aufgabe im Block **Aktion** die erforderliche Aktion an.

UNTERSUCHUNGSSTART MIT DEN RECHTEN EINES ANDEREN BENUTZERS

Die Untersuchungsaufgaben werden standardmäßig unter dem Benutzerkonto gestartet, mit dessen Rechten Sie sich im System angemeldet haben. Es kann aber erforderlich sein, eine Aufgabe mit den Rechten eines anderen Benutzers zu starten. Sie können das Benutzerkonto festlegen, mit dessen Rechten eine Untersuchungsaufgabe gestartet werden soll.

Gehen Sie folgendermaßen vor, um die Untersuchung mit den Rechten eines anderen Benutzers zu starten:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Seite des Fensters im Abschnitt **Untersuchung des Computers** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Schnelle Untersuchung**, **Untersuchung von Objekten** oder **Schwachstellensuche**).
4. Klicken Sie für die ausgewählte Aufgabe im Block **Startmodus** auf **Einstellungen**.
5. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Benutzer** das Kontrollkästchen **Aufgabe starten mit Rechten des Benutzers**. Geben Sie darunter in den Feldern den Benutzernamen und das Kennwort an.

TYP DER ZU UNTERSUCHENDEN OBJEKTE ÄNDERN

Durch die Angabe des Typs der zu untersuchenden Objekte bestimmen Sie das Format und die Größe der Dateien, die beim Ausführen der gewählten Aufgabe untersucht werden sollen.

Bei der Auswahl des Dateityps muss Folgendes beachtet werden:

- Es gibt eine Reihe von Dateiformaten (z.B. txt), für die das Risiko des Eindringens von schädlichem Code und dessen späterer Aktivierung relativ gering ist. Gleichzeitig gibt es Formate, die ausführbaren Code enthalten oder enthalten können (exe, dll, doc). Das Risiko, dass schädlicher Code in solche Dateien eindringt und aktiviert wird, ist relativ hoch.

- Ein Angreifer kann einen Virus in einer ausführbaren Datei, die in eine txt-Datei umbenannt wurde, an Ihren Computer senden. Wenn die Sie Untersuchung von Dateien nach Erweiterung gewählt haben, wird eine solche Datei bei der Untersuchung übersprungen. Wurde die Untersuchung von Dateien nach Format gewählt wurde, ignoriert Datei-Anti-Virus die Erweiterung und analysiert die Kopfzeile der Datei, wodurch sich ergeben kann, dass die Datei das Format exe besitzt. Eine solche Datei wird der sorgfältigen Virusuntersuchung unterzogen.

Gehen Sie folgendermaßen vor, um den Typ der zu untersuchenden Dateien zu ändern:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung des Computers** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Schnelle Untersuchung** oder **Untersuchung von Objekten**).
4. Klicken Sie für die ausgewählte Aufgabe im Block **Sicherheitsstufe** auf **Einstellungen**.
5. Wählen Sie im folgenden Fenster auf der Registerkarte **Gültigkeitsbereich** im Block **Dateitypen** die gewünschte Variante.

UNTERSUCHUNG VON ZUSAMMENGESETZTEN DATEIEN

Eine häufige Methode zum Verstecken von Viren ist das Eindringen von Schädlingen in zusammengesetzte Dateien wie Archive, Datenbanken usw. Um Viren zu erkennen, die auf diese Weise versteckt wurden, muss eine zusammengesetzte Datei entpackt werden. Dadurch kann das Untersuchungstempo wesentlich sinken.

Für jeden Typ einer zusammengesetzten Datei können Sie auswählen, ob alle oder nur neue Dateien untersucht werden sollen. Verwenden Sie zur Auswahl den Link neben dem Namen des Objekts. Er verändert seinen Wert, wenn mit der linken Maustaste darauf geklickt wird. Wenn der Modus gewählt wurde, in dem nur neue und veränderte Dateien untersucht werden (s. S. 92), stehen die Links zur Auswahl aller oder nur neuer Dateien nicht zur Verfügung.

Außerdem können Sie festlegen, bis zu welcher maximalen Größe eine zusammengesetzte Datei untersucht werden soll. Zusammengesetzte Dateien, die den festgelegten Wert überschreiten, werden nicht untersucht.

Gehen Sie folgendermaßen vor, um Liste der zu untersuchenden zusammengesetzten Dateien zu ändern:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung des Computers** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Schnelle Untersuchung** oder **Untersuchung von Objekten**).
4. Klicken Sie für die ausgewählte Aufgabe im Block **Sicherheitsstufe** auf **Einstellungen**.
5. Wählen Sie im folgenden Fenster auf der Registerkarte **Gültigkeitsbereich** im Block **Untersuchung von zusammengesetzten Dateien** die Typen der zusammengesetzten Dateien, die untersucht werden sollen.

Gehen Sie folgendermaßen vor, um eine maximale Größe für zusammengesetzte Dateien festzulegen, die untersucht werden sollen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung des Computers** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Schnelle Untersuchung** oder **Untersuchung von Objekten**).

4. Klicken Sie für die ausgewählte Aufgabe im Block **Sicherheitsstufe** auf **Einstellungen**.

5. Klicken Sie im folgenden Fenster auf der Registerkarte **Gültigkeitsbereich** im Block **Untersuchung von zusammengesetzten Dateien** auf **Erweitert**.

6. Aktivieren Sie im folgenden Fenster **Zusammengesetzte Dateien** das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken** und legen Sie die maximale Größe für zu untersuchende Dateien fest.

Wenn umfangreiche Dateien aus Archiven extrahiert werden, erfolgt eine Untersuchung auch dann, wenn das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken** aktiviert ist.

UNTERSUCHUNG OPTIMIEREN

Sie können die Untersuchungszeit verkürzen und die Arbeitsgeschwindigkeit von Kaspersky PURE erhöhen. Das lässt sich erreichen, wenn nur neue Dateien und Dateien, die seit der letzten Analyse verändert wurden, untersucht werden. Dieser Untersuchungsmodus erstreckt sich auf gewöhnliche und zusammengesetzte Dateien.

Außerdem kann die Untersuchungsdauer für ein einzelnes Objekt beschränkt werden. Wenn eine Datei nicht innerhalb der vorgegebenen Zeit untersucht wurde, wird sie von der laufenden Untersuchung ausgeschlossen (außer Archiven und Dateien, die aus mehreren Objekten bestehen).

- *Gehen Sie folgendermaßen vor, damit nur neue und veränderte Dateien untersucht werden:*

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung des Computers** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Schnelle Untersuchung** oder **Untersuchung von Objekten**).

4. Klicken Sie für die ausgewählte Aufgabe im Block **Sicherheitsstufe** auf **Einstellungen**.

5. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Gültigkeitsbereich** im Block **Untersuchung optimieren** das Kontrollkästchen **Nur neue und veränderte Dateien untersuchen**.

- *Gehen Sie folgendermaßen vor, um die Untersuchungsdauer einzuschränken:*

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung des Computers** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Schnelle Untersuchung** oder **Untersuchung von Objekten**).

4. Klicken Sie für die ausgewählte Aufgabe im Block **Sicherheitsstufe** auf **Einstellungen**.

5. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Gültigkeitsbereich** im Block **Untersuchung optimieren** das Kontrollkästchen **Dateien überspringen, wenn Untersuchung länger als** und geben Sie die Untersuchungsdauer für eine einzelne Datei an.

WECHSELDATENTRÄGER BEIM ANSCHLIEßEN UNTERSUCHEN

In letzter Zeit treten vermehrt schädliche Objekte auf, die Schwachstellen des Betriebssystems ausnutzen, um sich über lokale Netzwerke und Wechseldatenträger auszubreiten. Kaspersky PURE bietet eine Funktion, mit der Wechseldatenträger untersucht werden können, wenn sie an den Computer angeschlossen werden.

- *Gehen Sie folgendermaßen vor, um die Funktion anzupassen, mit der Wechseldatenträger untersucht werden, wenn sie an den Computer angeschlossen werden:*

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung des Computers** den Unterabschnitt **Allgemeine Einstellungen** aus.

4. Wählen Sie im rechten Fensterbereich im Block **Wechseldatenträger beim Anschließen untersuchen** eine Aktion und begrenzen Sie bei Bedarf im Feld unten die Größe der zu untersuchenden Laufwerke.

VERKNÜPFUNG FÜR DEN AUFGABENSTART ERSTELLEN

Für den Schnellstart der Aufgaben zur vollständigen und schnellen Untersuchung sowie zur Schwachstellensuche ist im Programm die Möglichkeit vorgesehen, Verknüpfungen anzulegen. So kann die erforderliche Untersuchungsaufgabe gestartet werden, ohne das Programmhauptfenster oder das Kontextmenü zu öffnen.

Gehen Sie folgendermaßen vor, um eine Verknüpfung für den Start einer Untersuchungsaufgabe zu erstellen:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung des Computers** den Unterabschnitt **Allgemeine Einstellungen** aus.

4. Klicken Sie auf der rechten Seite des Fensters im Block **Schneller Aufgabenstart** neben dem entsprechenden Aufgabennamen (**Schnelle Untersuchung**, **Vollständige Untersuchung** oder **Schwachstellensuche**) auf **Verknüpfung erstellen**.

5. Geben Sie im folgenden Fenster an, wo und unter welchem Namen die Verknüpfung gespeichert werden soll. Standardmäßig wird die Verknüpfung unter dem Aufgabennamen im Ordner *Arbeitsplatz* des aktiven Computerbenutzers erstellt.

SUCHE NACH SCHWACHSTELLEN

Schwachstellen in einem Betriebssystem können auf Programmierungs- oder Organisationsfehler, unsichere Kennwörter, Malware-Aktionen u.a. zurückgehen. Im Rahmen der Schwachstellensuche wird das System analysiert und es wird in den Einstellungen des Betriebssystems und des Browsers nach Anomalien und Beschädigungen gesucht. Weiterhin findet eine Suche nach Schwachstellen bei den Diensten statt und es werden andere Schutzmaßnahmen getroffen.

Die Diagnose kann eine gewisse Zeit beanspruchen. Anschließend werden die gefundenen Probleme im Hinblick auf ihre Gefährlichkeit für das System analysiert.

Nach dem Start der Aufgabe zur Schwachstellensuche (s. S. 68) wird der Vorgang im Fenster **Schwachstellensuche** im Feld **Ende** angezeigt. Die bei der Untersuchung im System und in Programmen gefundenen Schwachstellen werden im gleichen Fenster auf den Registerkarten **Systemschwachstellen** und **Programme mit Schwachstellen** angezeigt.

Während die Virensuche ausgeführt wird, werden Informationen über ihre Ergebnisse im Bericht von Kaspersky PURE aufgezeichnet.

Wie für die Untersuchungsaufgaben kann auch für die Aufgabe zur Schwachstellensuche ein Startzeitplan erstellt, eine Liste der Untersuchungsobjekte angelegt (s. S. 88), ein Benutzerkonto gewählt (s. Abschnitt "Untersuchungsstart mit den Rechten eines anderen Benutzers" auf S. 90) und eine Verknüpfung für den schnellen Aufgabenstart erstellt werden. In der Grundeinstellung sind die auf dem Computer installierten Anwendungen als Untersuchungsobjekt gewählt.

UPDATE

Das Update der Datenbanken und Programm-Module von Kaspersky PURE gewährleistet den aktuellen Zustand Ihres Computerschutzes. Jeden Tag tauchen neue Viren, trojanische Programme und andere Malware auf. Informationen über Bedrohungen und entsprechende Neutralisierungsmethoden sind in den Datenbanken von Kaspersky PURE enthalten. Deshalb stellt die regelmäßige Aktualisierung des Programms einen sehr wichtigen Faktor für die Sicherheit Ihres Computers und die rechtzeitige Erkennung neuer Gefahren dar.

Für ein regelmäßiges Update ist eine gültige Programmlizenz erforderlich. Ohne Lizenz ist nur ein einmaliges Update möglich.

Die Aktualisierung des Programms umfasst den Download und die Installation folgender Elemente auf Ihren Computer:

- Datenbanken für Kaspersky PURE.

  Der Schutz der Informationen auf ihrem Computer basiert auf Datenbanken, die Beschreibungen von Bedrohungssignaturen und Netzwerkangriffen, sowie entsprechende Desinfektionsmethoden enthalten. Die Schutzkomponenten verwenden diese bei der Suche und Desinfektion gefährlicher Objekte auf Ihrem Computer. Die Datenbanken werden regelmäßig durch Einträge über neue Bedrohungen und entsprechende Desinfektionsmethoden ergänzt. Deshalb wird ausdrücklich empfohlen, die Datenbanken regelmäßig zu aktualisieren.

  Gemeinsam mit den Datenbanken von Kaspersky PURE werden auch die Netzwerktreiber aktualisiert, die die Funktionalität für das Abfangen des Netzwerkverkehrs durch die Schutzkomponenten gewährleisten.

- Programm-Module.

  Neben den Datenbanken von Kaspersky PURE können auch die Programm-Module aktualisiert werden. Updatepakete beheben Schwachstellen von Kaspersky PURE, fügen neue Funktionen hinzu und optimieren bestehende Funktionen.

Die wichtigste Updatequelle für Kaspersky PURE sind spezielle Updateserver von Kaspersky Lab. Parallel zur Aktualisierung von Kaspersky PURE können Sie die Updates für Datenbanken und Programm-Module, die von den Kaspersky-Lab-Servern heruntergeladen werden, in einen lokalen Ordner kopieren, auf den dann andere Netzwerkcomputer zugreifen können. Dadurch lässt sich Internet-Traffic einsparen.

Zusätzlich können die Parameter für den automatischen Start des Updates angepasst werden.

Um Updates erfolgreich von den Servern herunterzuladen, muss Ihr Computer mit dem Internet verbunden sein. In der Grundeinstellung wird die Internetverbindung automatisch ermittelt. Wenn Sie einen Proxyserver verwenden, kann es notwendig sein, die Parameter der Verbindung anzupassen.

Bei der Aktualisierung werden die auf Ihrem Computer installierten Programm-Module und Datenbanken mit der aktuellen Version in der Updatequelle verglichen. Wenn Datenbanken und Module nicht aktuell sind, werden fehlende Teile der Updates auf Ihrem Computer installiert.

Wenn die Datenbanken stark veraltet sind, kann das Updatepaket relativ umfangreich sein und zusätzlichen Internet-Datenverkehr verursachen (bis zu mehreren Dutzend Megabyte).

Bevor die Datenbanken aktualisiert werden, legt Kaspersky PURE eine Sicherungskopie an. Bei Bedarf können Sie zur vorhergehenden Version der Datenbanken zurückkehren (s. Abschnitt "Rollback zum vorherigen Update" auf S. 98).

Informationen über den aktuellen Status der Datenbanken von Kaspersky PURE werden im Abschnitt **Update** des Fensters **Computersicherheit** angezeigt.

Informationen über die Updateergebnisse und über alle Ereignisse, die bei der Ausführung einer Updateaufgabe auftreten, werden im Bericht von Kaspersky PURE protokolliert.

IN DIESEM ABSCHNITT

Updatequelle auswählen 95

Zeitplan für Updatestart erstellen 97

Rollback zum vorherigen Update 98

Untersuchung der Quarantäne nach dem Update 98

Proxyserver verwenden 98

Updatestart mit den Rechten eines anderen Benutzers 99

UPDATEQUELLE AUSWÄHLEN

Eine *Updatequelle* ist eine Ressource, die Updates der Datenbanken und der Module für Kaspersky PURE enthält. Als Updatequelle können HTTP- oder FTP-Server, lokale Ordner oder Netzwerkordner angegebenen werden.

Als primäre Updatequelle dienen die Kaspersky-Lab-Updateserver, auf denen Updates der Datenbanken und Programm-Module für alle Kaspersky-Lab-Produkte zur Verfügung gestellt werden.

Wenn Sie keinen Zugriff auf die Kaspersky-Lab-Updateserver besitzen (wenn beispielsweise der Internetzugang eingeschränkt ist), können Sie sich an unsere Zentrale (http://www.kaspersky.de/kontakt) wenden. Dort können Sie die Adressen der Partner von Kaspersky Lab erfahren, die Ihnen die Updates auf einem Wechseldatenträger anbieten können.

Geben Sie zur Bestellung von Updates auf Wechseldatenträgern unbedingt an, ob Sie Updates für die Programm-Module erhalten möchten.

In der Grundeinstellung enthält die Liste nur die Kaspersky-Lab-Updateserver. Wenn mehrere Ressourcen als Updatequellen gewählt wurden, greift Kaspersky PURE bei der Aktualisierung genau nach der Liste darauf zu und aktualisiert sich von der ersten verfügbaren Quelle.

Wenn Sie als Updatequelle eine Ressource gewählt haben, die sich außerhalb des lokalen Netzwerks befindet, ist für die Aktualisierung eine Internetverbindung erforderlich.

➧ *Gehen Sie folgendermaßen vor, um eine Updatequelle auszuwählen:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Update** den Abschnitt **Update-Einstellungen**.
4. Klicken Sie auf der rechten Fensterseite im Block **Updatequelle** auf **Einstellungen**.
5. Klicken Sie im folgenden Fenster auf der Registerkarte **Quelle** auf den Link **Hinzufügen**, um das Fenster **Updatequelle auswählen** zu öffnen.
6. Wählen Sie einen Ordner aus, der die Updates enthält, oder geben Sie im Feld **Quelle** die Adresse des Servers ein, von dem die Updates heruntergeladen werden sollen.

IN DIESEM ABSCHNITT

Region des Updateservers wählen 96

Update aus dem gemeinsamen Ordner 96

REGION DES UPDATESERVERS WÄHLEN

Wenn Sie die Kaspersky-Lab-Server als Updatequelle verwenden, kann der für Sie günstigste Serverstandort für den Update-Download gewählt werden. Kaspersky Lab verfügt in mehreren Ländern der Erde über Server.

Durch die Verwendung des geografisch am nächsten gelegenen Kaspersky-Lab-Updateservers kann sich die Dauer des Update-Downloads verkürzen und das Übertragungstempo erhöhen. In der Grundeinstellung werden Informationen über den aktuellen Standort aus der Registrierung des Betriebssystems verwendet. Sie können die Region manuell wählen.

Gehen Sie folgendermaßen vor, um die Region des Servers zu wählen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Update** den Abschnitt **Update-Einstellungen**.
4. Klicken Sie auf der rechten Fensterseite im Block **Updatequelle** auf **Einstellungen**.
5. Wählen Sie im folgenden Fenster auf der Registerkarte **Quelle** im Block **Regionsoptionen** die Variante **Aus der Liste wählen** und wählen Sie aus der Dropdown-Liste das Land aus, in dem Sie sich gegenwärtig aufhalten.

UPDATE AUS DEM GEMEINSAMEN ORDNER

Um Internet-Datenverkehr einzusparen, kann festgelegt werden, dass Kaspersky PURE auf den Netzwerkcomputern aus einem gemeinsamen Ordner aktualisiert werden soll. In diesem Fall lädt ein Computer des Netzwerks das Updatepaket von den Kaspersky-Lab-Servern im Internet oder von einer anderen Webressource, auf der sich die aktuellen Updates befinden, herunter. Die heruntergeladenen Updates werden in einem gemeinsamen Ordner abgelegt, auf den die anderen Netzwerkcomputer zugreifen, um die Updates für Kaspersky PURE zu erhalten.

Gehen Sie folgendermaßen vor, um den Modus für die Update-Verteilung zu aktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Update** den Abschnitt **Update-Einstellungen**.
4. Aktivieren Sie im rechten Fensterbereich im Block **Erweitert** das Kontrollkästchen **Updates in folgenden Ordner kopieren** und geben Sie darunter im Feld den Pfad des gemeinsamen Ordners an, in dem heruntergeladene Updates abgelegt werden sollen. Außerdem kann mit Hilfe der Schaltfläche **Durchsuchen** ein Ordner gewählt werden.

Gehen Sie folgendermaßen vor, damit der Computer aus dem gewählten gemeinsamen Ordner aktualisiert wird:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Update** den Abschnitt **Update-Einstellungen**.
4. Klicken Sie auf der rechten Fensterseite im Block **Updatequelle** auf **Einstellungen**.

5. Klicken Sie im folgenden Fenster auf der Registerkarte **Quelle** auf den Link **Hinzufügen**, um das Fenster **Updatequelle auswählen** zu öffnen.

6. Wählen Sie einen Ordner aus oder geben im Feld **Quelle** einen vollständigen Ordnerpfad an.

7. Deaktivieren Sie auf der Registerkarte **Quelle** das Kontrollkästchen **Kaspersky-Lab-Updateserver**.

ZEITPLAN FÜR UPDATESTART ERSTELLEN

Es kann ein Zeitplan für den automatischen Start einer Updateaufgabe angelegt werden: In diesem werden eine Frequenz für den Aufgabenstart, ein Startzeitpunkt (falls erforderlich) sowie zusätzliche Parameter festgelegt.

Wenn der Aufgabenstart aus irgendeinem Grund nicht möglich war (wenn beispielsweise der Computer im betreffenden Moment ausgeschaltet war), können Sie festlegen, dass der Start einer übersprungenen Aufgabe automatisch zum nächstmöglichen Zeitpunkt erfolgt.

Außerdem können Sie den automatischen Aufgabenstart nach dem Start des Programms aufschieben. Dann werden alle geplanten Aufgaben erst gestartet, nachdem Kaspersky PURE gestartet wurde und eine bestimmte Zeit verstrichen ist.

- *Gehen Sie folgendermaßen vor, um den Startzeitplan für die Updateaufgabe anzupassen:*

  1. Öffnen Sie das Programmhauptfenster.

  2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

  3. Wählen Sie auf der linken Fensterseite im Abschnitt **Update** den Abschnitt **Update-Einstellungen**.

  4. Klicken Sie auf der rechten Fensterseite im Block **Startmodus** auf **Einstellungen**.

  5. Wählen Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Zeitplan** die Option **Nach Zeitplan**aus und konfigurieren Sie den Startmodus für die Aktualisierung.

- *Gehen Sie folgendermaßen vor, um den automatischen Start einer übersprungenen Aufgabe zu aktivieren:*

  1. Öffnen Sie das Programmhauptfenster.

  2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

  3. Wählen Sie auf der linken Fensterseite im Abschnitt **Update** den Abschnitt **Update-Einstellungen**.

  4. Klicken Sie auf der rechten Fensterseite im Block **Startmodus** auf **Einstellungen**.

  5. Wählen Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Zeitplan** die Option **Nach Zeitplan** aus und aktivieren Sie das Kontrollkästchen **Übersprungene Aufgaben starten**.

- *Gehen Sie folgendermaßen vor, um den Aufgabenstart nach dem Programmstart aufzuschieben:*

  1. Öffnen Sie das Programmhauptfenster.

  2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

  3. Wählen Sie auf der linken Fensterseite im Abschnitt **Update** den Abschnitt **Update-Einstellungen**.

  4. Klicken Sie auf der rechten Fensterseite im Block **Startmodus** auf **Einstellungen**.

  5. Wählen Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Zeitplan** die Option **Nach Zeitplan** aus und legen Sie im Feld **Start nach Programmstart aufschieben für** fest, wie lange der Aufgabenstart zurückgestellt werden soll.

ROLLBACK ZUM VORHERIGEN UPDATE

Nach dem ersten Update der Datenbanken und der Programm-Module von Kaspersky PURE steht Ihnen die Funktion des Rollback zu den Vorversionen der Datenbanken zur Verfügung.

Jedes Mal, wenn Sie das Update starten, erstellt Kaspersky PURE zuerst eine Sicherungskopie der bisher verwendeten Datenbanken und Programm-Module und beginnt danach mit der Aktualisierung. Dadurch wird Ihnen erlaubt, bei Bedarf zur Verwendung der vorherigen Datenbanken zurückzukehren. Die Rollback-Funktion ist beispielsweise nützlich, wenn die neue Datenbankversion eine fehlerhafte Signatur enthält, die dazu führt, dass Kaspersky PURE ein harmloses Programm blockiert.

Wenn die Datenbanken von Kaspersky PURE beschädigt sind, wird empfohlen, die Updateaufgabe zu starten, um funktionsfähige aktuelle Datenbanken herunterzuladen.

Gehen Sie folgendermaßen vor, um zur Verwendung der vorhergehenden Version der Datenbanken zurückzukehren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.

   Das Fenster **Computersicherheit** wird geöffnet.

2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update**.

3. Klicken Sie auf der rechten Fensterseite auf **Rollback zu den vorherigen Datenbanken**.

UNTERSUCHUNG DER QUARANTÄNE NACH DEM UPDATE

Wenn sich bei der Untersuchung nicht genau ermitteln lässt, von welchen Schadprogrammen ein Objekt infiziert ist, wird es in die Quarantäne verschoben. Eine Bedrohung kann möglicherweise eindeutig bestimmt und desinfiziert werden, nachdem die Datenbanken aktualisiert wurden. Sie können eine automatische Untersuchung der Quarantäneobjekte nach jedem Update festlegen.

Es wird empfohlen, die Objekte in der Quarantäne regelmäßig zu überprüfen. Aufgrund der Untersuchung kann sich ihr Status ändern. Bestimmte Objekte können am ursprünglichen Ort wiederhergestellt und wieder verwendet werden.

Gehen Sie folgendermaßen vor, um festzulegen, dass die Quarantänedateien nach einem Update automatisch untersucht werden:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie auf der linken Fensterseite im Abschnitt **Update** den Abschnitt **Update-Einstellungen**.

4. Aktivieren Sie im rechten Fensterbereich im Block **Erweitert** das Kontrollkästchen **Quarantänedateien nach jedem Update untersuchen**.

PROXYSERVER VERWENDEN

Wenn die Internetverbindung über einen Proxyserver erfolgt, müssen seine Parameter angepasst werden, um eine korrekte Aktualisierung von Kaspersky PURE zu ermöglichen.

Gehen Sie folgendermaßen vor, um die Proxyserver-Parameter anzupassen:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie auf der linken Fensterseite im Abschnitt **Update** den Abschnitt **Update-Einstellungen**.

4. Klicken Sie auf der rechten Fensterseite im Block **Updatequelle** auf **Einstellungen**.

5. Klicken Sie im folgenden Fenster auf der Registerkarte **Quelle** auf **Proxyserver**.

6. Passen Sie im folgenden Fenster **Proxyserver-Einstellungen** die Parameter für den Proxyserver an.

UPDATESTART MIT DEN RECHTEN EINES ANDEREN BENUTZERS

Das Update wird standardmäßig unter dem Benutzerkonto gestartet, mit dessen Rechten Sie sich im System angemeldet haben. Das Update für Kaspersky PURE kann aber auch aus einer Quelle erfolgen, auf die Sie keinen Zugriff besitzen (z.B. Netzwerkordner, der Updates enthält) oder für die Sie nicht über Rechte eines autorisierten Benutzers für den Proxyserver verfügen. Sie können das Update von Kaspersky PURE unter dem Namen eines Benutzers starten, der über die erforderlichen Privilegien verfügt.

Gehen Sie folgendermaßen vor, um das Update mit den Rechten eines anderen Benutzers zu starten:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie auf der linken Fensterseite im Abschnitt **Update** den Abschnitt **Update-Einstellungen**.

4. Klicken Sie auf der rechten Fensterseite im Block **Startmodus** auf **Einstellungen**.

5. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Benutzer** das Kontrollkästchen **Aufgabe starten mit Rechten des Benutzers**. Geben Sie darunter in den Feldern den Benutzernamen und das Kennwort an.

DATEI-ANTI-VIRUS

Datei-Anti-Virus erlaubt es, das Dateisystem des Computers vor einer Infektion zu schützen. Die Komponente wird beim Hochfahren des Betriebssystems gestartet, befindet sich ständig im Arbeitsspeicher des Computers und untersucht alle Dateien, die auf Ihrem Computer und auf allen angeschlossenen Laufwerken geöffnet, gespeichert und gestartet werden.

Wenn ein Benutzer oder ein Programm auf eine Datei zugreift, prüft Datei-Anti-Virus, ob die Datenbanken iChecker und iSwift Informationen über die Datei enthalten, und entscheidet auf Basis dieser Informationen, ob eine Untersuchung der Datei erforderlich ist.

Die Spezialisten von Kaspersky Lab warnen davor, die Funktionsparameter von Datei-Anti-Virus zu verändern. In den meisten Fällen ist es ausreichend, die Sicherheitsstufe zu ändern.

Für Fälle, in denen die Untersuchung des Dateisystem vorübergehend deaktiviert werden soll, können Sie das automatische Anhalten von Datei-Anti-Virus einstellen. Bei Bedarf können Sie die Komponente deaktivieren.

Sie können einen Schutzbereich anlegen und einen Untersuchungsmodus für Objekte auswählen.

Standardmäßig ist immer der Modus zur Untersuchung mit Hilfe der Einträge der Programm-Datenbanken aktiviert. Außerdem können heuristische Analyse (s. S. 103) und unterschiedliche Untersuchungstechnologien (s. S. 104) eingesetzt werden.

Beim Fund einer Bedrohung weist Kaspersky PURE dem gefundenen Objekt eine der folgenden Statusvarianten zu:

- Status eines der schädlichen Programme (beispielsweise *Virus*, *trojanisches Programm*).

- Status *möglicherweise infiziert* (verdächtig) wenn sich aufgrund der Untersuchung nicht eindeutig feststellen lässt, ob das Objekt infiziert ist oder nicht. Möglicherweise enthält die Datei eine virentypische Codefolge oder den modifizierten Code eines bekannten Virus.

Anschließend zeigt das Programm auf dem Bildschirm eine Meldung (s. S. 244) über die gefundene Bedrohung an und führt die festgelegte Aktion aus. Sie können die Aktion beim Fund einer Bedrohung ändern.

Wenn Sie im automatischen Modus (s. Abschnitt "Interaktiven Schutzmodus verwenden" auf S. 61), wendet Kaspersky PURE beim Fund gefährlicher Objekte automatisch die von Kaspersky Lab empfohlene Aktion an. Für schädliche Objekte ist dies die Aktion **Desinfizieren. Löschen, wenn Desinfektion nicht möglich**, für verdächtige – **In die Quarantäne verschieben**. Wenn Sie im interaktiven Modus arbeiten (s. Abschnitt "Interaktiven Schutzmodus verwenden" auf S. 61), zeigt das Programm beim Fund gefährlicher Objekte auf dem Bildschirm eine Meldung an, in der Sie eine Aktion auswählen können.

Bevor ein infiziertes Objekt desinfiziert oder gelöscht wird, legt Kaspersky PURE eine Sicherungskopie des Objekts an. Dadurch wird erlaubt, das Objekt bei Bedarf wiederherzustellen oder später zu desinfizieren. Verdächtige (möglicherweise infizierte) Objekte werden in die Quarantäne verschoben. Sie können eine automatische Untersuchung der Quarantänedateien nach jedem Update festlegen.

IN DIESEM ABSCHNITT

Datei-Anti-Virus aktivieren und deaktivieren 100

Datei-Anti-Virus automatisch anhalten 100

Schutzbereich festlegen 101

Sicherheitsstufe ändern und wiederherstellen 102

Untersuchungsmodus ändern 103

Heuristische Analyse verwenden 103

Untersuchungstechnologie 104

Aktion für gefundene Objekte ändern 104

Untersuchung von zusammengesetzten Dateien 104

Untersuchung optimieren 105

DATEI-ANTI-VIRUS AKTIVIEREN UND DEAKTIVIEREN

Datei-Anti-Virus ist standardmäßig aktiviert und arbeitet im optimalen Modus. Bei Bedarf kann Datei-Anti-Virus deaktiviert werden.

Gehen Sie folgendermaßen vor, um Datei-Anti-Virus zu aktivieren oder zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
4. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Datei-Anti-Virus aktivieren**, um die Komponente auszuschalten. Aktivieren Sie dieses Kontrollkästchen, um die Komponente einzuschalten.

DATEI-ANTI-VIRUS AUTOMATISCH ANHALTEN

Bei der Ausführung von Arbeiten, die die Betriebssystemressourcen stark beanspruchen, kann die Arbeit von Datei-Anti-Virus vorübergehend angehalten werden. Um die Belastung zu verringern und den schnellen Zugriff auf Objekte zu

gewährleisten, kann festgelegt werden, dass die Komponente zu einem bestimmten Zeitpunkt oder bei der Arbeit mit bestimmten Programmen automatisch angehalten wird.

Das Anhalten von Datei-Anti-Virus bei einem Konflikt mit bestimmten Programmen gilt als Notlösung! Sollten bei der Arbeit der Komponente Konflikte auftreten, dann wenden Sie sich an den Technischen Support von Kaspersky Lab (http://support.kaspersky.de). Die Spezialisten helfen Ihnen dabei, auf Ihrem Computer die gemeinsame Arbeit von Kaspersky PURE mit anderen Programmen einzurichten.

Gehen Sie folgendermaßen vor, damit die Komponente zu einem bestimmten Zeitpunkt angehalten wird:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
5. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Aufgabe anhalten** das Kontrollkästchen **Nach Zeitplan** und klicken Sie auf **Zeitplan**.
6. Legen Sie im Fenster **Aufgabe anhalten** (in den Feldern **Anhalten um** und **Fortsetzen um**) den Zeitraum fest, für den der Schutz angehalten werden soll (im Format HH:MM).

Gehen Sie folgendermaßen vor, damit die Komponente beim Start bestimmter Programme angehalten wird:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
5. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Aufgabe anhalten** das Kontrollkästchen Beim **Start bestimmter Anwendungen** und klicken Sie auf **Auswählen**.
6. Legen Sie im Fenster **Programme** die Liste der Programme an, bei deren Arbeit die Komponente angehalten werden soll.

SCHUTZBEREICH FESTLEGEN

Der Begriff Schutzbereich umfasst den Ort der Untersuchungsobjekte und den Typ der zu untersuchenden Dateien. Kaspersky PURE untersucht standardmäßig nur potentiell infizierbare Dateien, die von beliebigen Festplatten, Wechseldatenträgern und Netzlaufwerken aus gestartet werden.

Sie können den Schutzbereich erweitern oder einschränken, indem Sie Untersuchungsobjekte hinzufügen / entfernen oder den Typ der zu untersuchenden Dateien ändern. Es können beispielsweise nur exe-Dateien, die von Netzlaufwerken aus gestartet werden, zur Untersuchung gewählt werden.

Bei der Auswahl des Dateityps muss Folgendes beachtet werden:

- Es gibt eine Reihe von Dateiformaten (z.B. txt), für die das Risiko des Eindringens von schädlichem Code und dessen späterer Aktivierung relativ gering ist. Gleichzeitig gibt es Formate, die ausführbaren Code enthalten oder enthalten können (exe, dll, doc). Das Risiko, dass schädlicher Code in solche Dateien eindringt und aktiviert wird, ist relativ hoch.
- Ein Angreifer kann einen Virus in einer ausführbaren Datei, die in eine txt-Datei umbenannt wurde, an Ihren Computer senden. Wenn die Sie Untersuchung von Dateien nach Erweiterung gewählt haben, wird eine solche Datei bei der Untersuchung übersprungen. Wurde die Untersuchung von Dateien nach Format gewählt wurde,

ignoriert Datei-Anti-Virus die Erweiterung und analysiert die Kopfzeile der Datei, wodurch sich ergeben kann, dass die Datei das Format exe besitzt. Eine solche Datei wird der sorgfältigen Virusuntersuchung unterzogen.

Gehen Sie folgendermaßen vor, um die Liste der Untersuchungsobjekte zu ändern:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
5. Klicken Sie im folgenden Fenster auf der Registerkarte **Allgemein** im Block **Schutzbereich** auf den Link **Hinzufügen**, um das Fenster zur Objektauswahl zu öffnen.
6. Wählen Sie im Fenster **Untersuchungsobjekt wählen** ein Objekt und klicken Sie auf **Hinzufügen**.
7. Nachdem alle erforderlichen Objekte hinzugefügt wurden, klicken Sie im Fenster **Untersuchungsobjekt auswählen** auf **OK**.
8. Um ein Objekt aus der Untersuchungsliste auszuschließen, deaktivieren Sie das entsprechende Kontrollkästchen.

Gehen Sie folgendermaßen vor, um den Typ der zu untersuchenden Dateien zu ändern:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
5. Wählen Sie im folgenden Fenster auf der Registerkarte **Allgemein** im Block **Dateitypen** den gewünschten Parameter.

SICHERHEITSSTUFE ÄNDERN UND WIEDERHERSTELLEN

Abhängig von den aktuellen Erfordernissen können Sie eine vordefinierte Stufe für die Sicherheit von Dateien und Speicher wählen oder die Einstellungen von Datei-Anti-Virus entsprechend anpassen.

Während der Konfiguration einer Komponente können Sie jederzeit zu den empfohlenen Einstellungen zurückkehren. Diese Werte gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und entsprechen der Sicherheitsstufe **Empfohlen**.

Es wird empfohlen, vor der Auswahl der niedrigen Sicherheitsstufe die vollständige Untersuchung des Computers mit der hohen Sicherheitsstufe vorzunehmen (s. Abschnitt "Wie eine vollständige Virenuntersuchung des Computers ausgeführt wird" auf S. 68).

Gehen Sie folgendermaßen vor, um die festgelegte Sicherheitsstufe für Dateien und Speicher zu ändern:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
4. Stellen Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** die erforderliche Sicherheitsstufe ein oder klicken Sie auf **Einstellungen**, um die Untersuchungseinstellungen manuell anzupassen.

Wenn manuelle Änderungen erfolgen, ändert sich der Name der Sicherheitsstufe in **Benutzerdefiniert**.

Gehen Sie folgendermaßen vor, um die standardmäßigen Schutzeinstellungen wiederherzustellen,

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Standard**.

UNTERSUCHUNGSMODUS ÄNDERN

Unter Untersuchungsmodus wird die Bedingung für das Auslösen von Datei-Anti-Virus verstanden. In der Grundeinstellung verwendet Kaspersky PURE den intelligenten Modus, in dem die Entscheidung über die Untersuchung eines Objekts auf Basis der Operationen, die damit ausgeführt werden sollen, gefällt wird. Beispielsweise untersucht Kaspersky PURE bei der Arbeit mit einem Microsoft Office-Dokument eine Datei, wenn sie zum ersten Mal geöffnet und zum letzten Mal geschlossen wird. Alle dazwischen liegenden Operationen, bei denen die Datei verändert wird, werden von der Untersuchung ausgeschlossen.

Sie können den Untersuchungsmodus für Objekte ändern. Der passende Modus ist davon abhängig, mit welcher Art von Dateien Sie überwiegend arbeiten.

Gehen Sie folgendermaßen vor, um den Untersuchungsmodus für Objekte zu ändern:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
5. Wählen Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Untersuchungsmodus** den erforderlichen Modus.

HEURISTISCHE ANALYSE VERWENDEN

Bei der Arbeit von Datei-Anti-Virus wird immer die Methode *Signaturanalyse* verwendet, bei der Kaspersky PURE ein gefundenes Objekt mit den Einträgen in den Datenbanken vergleicht.

Um die Effektivität des Schutzes zu steigern, können Sie eine *heuristische Analyse* verwenden (Analyse der Aktivität, die ein Objekt im System zeigt). Diese Analyse erlaubt die Erkennung neuer Schadobjekte, über die noch keine Datenbankeinträge vorliegen.

Gehen Sie folgendermaßen vor, um die Verwendung der heuristischen Analyse zu aktivieren oder zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
5. Aktivieren Sie im folgenden Fenster **Leistung** im Block **Untersuchungsmethoden** das Kontrollkästchen **Heuristische Analyse** und stellen Sie darunter die Genauigkeitsstufe der Untersuchung ein. Deaktivieren Sie das Kontrollkästchen **Heuristische Analyse**, wenn diese Untersuchungsmethode nicht verwendet werden soll.

UNTERSUCHUNGSTECHNOLOGIE

Zusätzlich zur heuristischen Analyse können Sie spezielle Technologien einsetzen, mit denen das Tempo der Objektuntersuchung gesteigert werden kann. Dabei werden Dateien ausgeschlossen, die seit dem letzten Scan nicht verändert wurden.

Gehen Sie folgendermaßen vor, um die Technologien zur Objektuntersuchung zu aktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
5. Wählen Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Untersuchungstechnologien** die gewünschten Werte.

AKTION FÜR GEFUNDENE OBJEKTE ÄNDERN

Programm eine Aktion aus. Das Vorgehen ist davon abhängig, ob der automatische oder interaktive Modus ausgewählt wurde (s. Abschnitt "Datei-Anti-Virus" auf S. 99). Sie können die vordefinierte Aktion ändern.

Gehen Sie folgendermaßen vor, um die festgelegte Aktion für gefundene Objekte zu ändern:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
4. Wählen Sie auf der rechten Fensterseite im Block **Aktion** die entsprechende Variante.

UNTERSUCHUNG VON ZUSAMMENGESETZTEN DATEIEN

Eine häufige Methode zum Verstecken von Viren ist das Eindringen von Schädlingen in zusammengesetzte Dateien wie Archive, Datenbanken usw. Um Viren zu erkennen, die auf diese Weise versteckt wurden, muss eine zusammengesetzte Datei entpackt werden. Dadurch kann das Untersuchungstempo wesentlich sinken.

Für jeden Typ einer zusammengesetzten Datei können Sie auswählen, ob alle oder nur neue Dateien untersucht werden sollen.

In der Grundeinstellung untersucht Kaspersky PURE nur angehängte OLE-Objekte. Installationspakete und Dateien, die OLE-Objekte enthalten, werden beim Öffnen ausgeführt und gelten deshalb als gefährlicher als Archive.

Bei der Untersuchung von umfangreichen zusammengesetzten Dateien kann das vorausgehende Entpacken viel Zeit beanspruchen. Diese Dauer kann reduziert werden, wenn die Untersuchung von Dateien, die eine bestimmte Größe überschreiten, im Hintergrundmodus erfolgt. Wenn bei der Arbeit mit einer solchen Datei ein schädliches Objekt gefunden wird, werden Sie von Kaspersky PURE darüber informiert.

Außerdem können Sie festlegen, bis zu welcher maximalen Größe eine zusammengesetzte Datei untersucht werden soll. Zusammengesetzte Dateien, die den festgelegten Wert überschreiten, werden nicht untersucht.

Gehen Sie folgendermaßen vor, um Liste der zu untersuchenden zusammengesetzten Dateien zu ändern:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.

4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.

5. Wählen Sie im folgenden Fenster auf der Registerkarte **Leistung** im Block **Untersuchung von zusammengesetzten Dateien** die Typen der zusammengesetzten Dateien, die untersucht werden sollen.

Gehen Sie folgendermaßen vor, um eine maximale Größe für zusammengesetzte Dateien festzulegen, die untersucht werden sollen:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.

4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.

5. Klicken Sie im folgenden Fenster auf der Registerkarte **Leistung** im Block **Untersuchung von zusammengesetzten Dateien** auf **Erweitert**.

6. Aktivieren Sie im Fenster **Zusammengesetzte Dateien** das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken** und legen Sie eine maximale Größe für zu untersuchende Dateien fest.

Wenn umfangreiche Dateien aus Archiven extrahiert werden, erfolgt eine Untersuchung auch dann, wenn das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken** aktiviert ist.

Gehen Sie folgendermaßen vor, damit umfangreiche zusammengesetzte Dateien im Hintergrundmodus entpackt werden:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.

4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.

5. Klicken Sie im folgenden Fenster auf der Registerkarte **Leistung** im Block **Untersuchung von zusammengesetzten Dateien** auf **Erweitert**.

6. Aktivieren Sie im Fenster **Zusammengesetzte Dateien** das Kontrollkästchen **Zusammengesetzte Dateien im Hintergrund entpacken** und legen Sie eine minimale Dateigröße fest.

UNTERSUCHUNG OPTIMIEREN

Sie können die Untersuchungszeit verkürzen und die Arbeitsgeschwindigkeit von Kaspersky PURE erhöhen. Das lässt sich erreichen, wenn nur neue Dateien und Dateien, die seit der letzten Analyse verändert wurden, untersucht werden. Dieser Untersuchungsmodus erstreckt sich auf gewöhnliche und zusammengesetzte Dateien.

Gehen Sie folgendermaßen vor, damit nur neue und veränderte Dateien untersucht werden:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.

4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.

5. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Leistung** im Block **Untersuchung optimieren** das Kontrollkästchen **Nur neue und veränderte Dateien untersuchen**.

MAIL-ANTI-VIRUS

Mail-Anti-Virus untersucht, ob in ein- und ausgehenden E-Mails gefährliche Objekte vorhanden sind. Diese Komponente wird beim Start des Betriebssystems gestartet, befindet sich ständig im Arbeitsspeicher des Computers und untersucht alle E-Mail-Nachrichten, die über die Protokolle POP3, SMTP, IMAP, MAPI und NNTP sowie über geschützte Verbindungen (SSL) über die Protokolle POP3 und IMAP übertragen werden (s. Abschnitt "Untersuchung geschützter Verbindungen" auf S. 157)..

Als Indikator für die Arbeit der Komponente dient das Symbol im Infobereich der Taskleiste, das jedes Mal bei der Untersuchung einer E-Mail das Aussehen annimmt.

Jede Nachricht, die von einem Benutzer empfangen oder gesendet wird, wird abgefangen und in ihre Bestandteile (Kopfzeile, Briefkörper, Anhänge) zerlegt. Der Briefkörper und die Anhänge einer Nachricht (einschließlich eingebetteten OLE-Objekten) werden auf Bedrohungen untersucht.

Die Spezialisten von Kaspersky Lab warnen davor, die Funktionsparameter von Mail-Anti-Virus zu verändern. In den meisten Fällen ist es ausreichend, eine Sicherheitsstufe auszuwählen (s. Abschnitt "Sicherheitsstufe ändern und wiederherstellen" auf S. 108).

Sie können angeben, welche Nachrichtentypen untersucht und welche Untersuchungsmethoden verwendet werden sollen. Standardmäßig ist immer der Modus zur Untersuchung mit Hilfe der Einträge der Programm-Datenbanken aktiviert. Zusätzlich kann die heuristische Analyse eingesetzt werden. Außerdem können Sie die Anlagenfilterung (s. S. 109) aktivieren, mit der Dateien bestimmter Typen automatisch umbenannt oder gelöscht werden können.

Beim Fund einer Bedrohung weist Kaspersky PURE dem gefundenen Objekt eine der folgenden Statusvarianten zu:

- Status eines der schädlichen Programme (beispielsweise *Virus*, *trojanisches Programm*).
- Status *möglicherweise infiziert* (verdächtig) wenn sich aufgrund der Untersuchung nicht eindeutig feststellen lässt, ob das Objekt infiziert ist oder nicht. Möglicherweise enthält die Datei eine virentypische Codefolge oder den modifizierten Code eines bekannten Virus.

Anschließend blockiert das Programm die Nachricht, zeigt auf dem Bildschirm eine Meldung (s. S. 244)über die gefundene Bedrohung an und führt die festgelegte Aktion aus. Sie können die Aktion beim Fund einer Bedrohung ändern (s. Abschnitt "Aktion für gefundene Objekte ändern" auf S. 109).

Wenn Sie im automatischen Modus (s. Abschnitt "Interaktiven Schutzmodus verwenden" auf S. 61), wendet Kaspersky PURE beim Fund gefährlicher Objekte automatisch die von Kaspersky Lab empfohlene Aktion an. Für schädliche Objekte ist dies die Aktion **Desinfizieren. Löschen, wenn Desinfektion nicht möglich**, für verdächtige – **In die Quarantäne verschieben**. Wenn Sie im interaktiven Modus arbeiten (s. Abschnitt "Interaktiven Schutzmodus verwenden" auf S. 61), zeigt das Programm beim Fund gefährlicher Objekte auf dem Bildschirm eine Meldung an, in der Sie eine Aktion auswählen können.

Bevor ein infiziertes Objekt desinfiziert oder gelöscht wird, legt Kaspersky PURE eine Sicherungskopie des Objekts an. Dadurch wird erlaubt, das Objekt bei Bedarf wiederherzustellen oder später zu desinfizieren. Verdächtige (möglicherweise infizierte) Objekte werden in die Quarantäne verschoben. Sie können eine automatische Untersuchung der Quarantänedateien nach jedem Update festlegen.

Bei erfolgreicher Desinfektion erhält der Benutzer Zugriff auf die E-Mail. Wenn die Desinfektion fehlschlägt, wird das infizierte Objekt aus der Nachricht gelöscht. Als Ergebnis der Antiviren-Bearbeitung wird in die Betreffzeile der E-Mail ein spezieller Text eingefügt, der darüber informiert, dass sie von Kaspersky PURE bearbeitet wurde.

Bei Bedarf können Sie Mail-Anti-Virus deaktivieren (s. Abschnitt "Mail-Anti-Virus aktivieren und deaktivieren" auf S. 107).

Für das Mailprogramm Microsoft Office Outlook ist ein integrierbares Erweiterungsmodul (s. Abschnitt "E-Mail-Untersuchung in Microsoft Office Outlook" auf S. 110) vorgesehen, das die Feineinstellung der E-Mail-Untersuchung erlaubt.

Wenn Sie das Mailprogramm The Bat! verwenden, kann Kaspersky PURE zusammen mit anderen Antiviren-Anwendungen benutzt werden. Dabei werden die Regeln zur Verarbeitung des Mailverkehrs (s. Abschnitt "E-Mail-Untersuchung in The Bat!" auf S. 110) direkt im Programm The Bat! erstellt und besitzen Vorrang gegenüber den Parametern für den E-Mail-Schutz des Programms.

Bei der Arbeit mit anderen Mailprogrammen (einschließlich Microsoft Outlook Express (Windows Mail), Mozilla Thunderbird, Eudora, Incredimail) untersucht Mail-Anti-Virus den Mailverkehr der Protokolle SMTP, POP3, IMAP und NNTP bei Empfang bzw. Versand.

Beachten Sie, dass bei der Arbeit mit dem Mailprogramm Thunderbird E-Mails, die mit dem IMAP- Protokoll übertragen werden, nicht auf Viren untersucht werden, wenn Filter verwendet werden, die Nachrichten aus dem Ordner **Posteingang** verschieben.

IN DIESEM ABSCHNITT

Mail-Anti-Virus aktivieren und deaktivieren 107

Schutzbereich festlegen 107

Sicherheitsstufe ändern und wiederherstellen..... 108

Heuristische Analyse verwenden 109

Aktion für gefundene Objekte ändern 109

Anlagenfilterung 109

Untersuchung von zusammengesetzten Dateien 110

E-Mail-Untersuchung in Microsoft Office Outlook..... 110

E-Mail-Untersuchung in The Bat! 110

MAIL-ANTI-VIRUS AKTIVIEREN UND DEAKTIVIEREN

Mail-Anti-Virus ist standardmäßig aktiviert und arbeitet im optimalen Modus. Bei Bedarf kann Mail-Anti-Virus deaktiviert werden.

Gehen Sie folgendermaßen vor, um Mail-Anti-Virus zu aktivieren oder zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Mail-Anti-Virus**.
4. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Mail-Anti-Virus aktivieren**, um die Komponente auszuschalten. Aktivieren Sie dieses Kontrollkästchen, um die Komponente einzuschalten.

SCHUTZBEREICH FESTLEGEN

Unter Schutzbereich wird der Typ der Nachrichten verstanden, die untersucht werden sollen. Standardmäßig untersucht Kaspersky PURE sowohl eingehende, als auch ausgehende E-Mails.

Wenn Sie nur die Untersuchung eingehender E-Mails gewählt haben, ist es empfehlenswert, zu Beginn der Arbeit mit Kaspersky PURE die ausgehenden E-Mails zu untersuchen, weil sich auf Ihrem Computer Mailwürmer befinden können, die E-Mails als Kanal verwenden, um sich weiterzuverbreiten. Dadurch wird erlaubt, Probleme zu verhindern, die mit dem unkontrollierten Versenden infizierter E-Mails von Ihrem Computer verbunden sind.

Zum Schutzbereich gehören auch die Parameter für die Integration von Mail-Anti-Virus in das System und die zu untersuchenden Protokolle. In der Grundeinstellung wird Mail-Anti-Virus in die Mailprogramme Microsoft Office Outlook und The Bat! integriert.

Gehen Sie folgendermaßen vor, um die Untersuchung ausgehender E-Mails auszuschalten:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Mail-Anti-Virus**.
4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
5. Wählen Sie im folgenden Fenster auf der Registerkarte **Allgemein** im Block **Schutzbereich** die Variante **Nur eingehende Nachrichten**.

Gehen Sie folgendermaßen vor, um die zu untersuchenden Protokolle und die Parameter für die Integration von Mail-Anti-Virus in das System festzulegen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Mail-Anti-Virus**.
4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
5. Wählen Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Integration ins System** die erforderlichen Parameter.

SICHERHEITSSTUFE ÄNDERN UND WIEDERHERSTELLEN

Abhängig von den aktuellen Erfordernissen können Sie eine vordefinierte Sicherheitsstufe für E-Mails wählen oder die Einstellungen von Mail-Anti-Virus entsprechend anpassen.

Während der Konfiguration einer Komponente können Sie jederzeit zu den empfohlenen Einstellungen zurückkehren. Diese Werte gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und entsprechen der Sicherheitsstufe **Empfohlen**.

Gehen Sie folgendermaßen vor, um die festgelegte Sicherheitsstufe für E-Mails zu ändern:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Mail-Anti-Virus**.
4. Stellen Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** die erforderliche Sicherheitsstufe ein oder klicken Sie auf **Einstellungen**, um die Untersuchungseinstellungen manuell anzupassen.

   Wenn manuelle Änderungen erfolgen, ändert sich der Name der Sicherheitsstufe in **Benutzerdefiniert**.

Gehen Sie folgendermaßen vor, um die standardmäßigen Einstellungen für den Mail-Schutz wiederherzustellen,

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Mail-Anti-Virus**.

4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Standard**.

HEURISTISCHE ANALYSE VERWENDEN

Bei der Arbeit von Mail-Anti-Virus wird immer die Methode *Signaturanalyse* verwendet, bei der Kaspersky PURE ein gefundenes Objekt mit den Einträgen in den Datenbanken vergleicht.

Um die Effektivität des Schutzes zu steigern, können Sie eine *heuristische Analyse* verwenden (Analyse der Aktivität, die ein Objekt im System zeigt). Diese Analyse erlaubt die Erkennung neuer Schadobjekte, über die noch keine Datenbankeinträge vorliegen.

Gehen Sie folgendermaßen vor, um die Verwendung der heuristischen Analyse zu aktivieren oder zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Mail-Anti-Virus**.
4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
5. Aktivieren Sie im folgenden Fenster **Allgemein** im Block **Untersuchungsmethoden** das Kontrollkästchen **Heuristische Analyse** und stellen Sie darunter die Genauigkeitsstufe der Untersuchung ein. Deaktivieren Sie das Kontrollkästchen **Heuristische Analyse**, wenn diese Untersuchungsmethode nicht verwendet werden soll.

AKTION FÜR GEFUNDENE OBJEKTE ÄNDERN

Beim Fund infizierter oder möglicherweise infizierter Objekte führt das Programm eine Aktion aus. Das Vorgehen ist davon abhängig, ob der automatische oder interaktive Modus ausgewählt wurdeй (s. Abschnitt "Mail-Anti-Virus" auf S. 106). Sie können die vordefinierte Aktion ändern.

Gehen Sie folgendermaßen vor, um die festgelegte Aktion für gefundene Objekte zu ändern:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Mail-Anti-Virus**.
4. Wählen Sie auf der rechten Fensterseite im Block **Aktion** die entsprechende Variante.

ANLAGENFILTERUNG

Schädliche Programme werden am häufigsten als Anhänge einer Nachricht verbreitet. Um den Computer beispielsweise davor zu schützen, dass angehängte Dateien automatisch gestartet werden, können Sie die Anlagenfilterung aktivieren. Sie erlaubt es, Dateien bestimmter Typen automatisch umzubenennen oder zu löschen.

Gehen Sie folgendermaßen vor, um die Anlagenfilterung zu aktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Mail-Anti-Virus**.
4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.

5. Wählen Sie im folgenden Fenster auf der Registerkarte **Anlagenfilterung** einen Filtermodus. Bei Auswahl der letzten beiden Modi wird die Liste der Dateitypen (Erweiterungen) aktiviert. In dieser Liste können Sie die erforderlichen Typen wählen oder die Maske eines neuen Typs hinzufügen.

   Um der Liste die Maske eines neuen Typs hinzuzufügen, öffnen Sie mit dem Link **Hinzufügen** das Fenster **Maske für einen Dateinamen** und geben Sie dort die erforderlichen Daten ein.

UNTERSUCHUNG VON ZUSAMMENGESETZTEN DATEIEN

Eine häufige Methode zum Verstecken von Viren ist das Eindringen von Schädlingen in zusammengesetzte Dateien wie Archive, Datenbanken usw. Um Viren zu erkennen, die auf diese Weise versteckt wurden, muss eine zusammengesetzte Datei entpackt werden. Dadurch kann das Untersuchungstempo wesentlich sinken.

Sie können die Untersuchung angehängter Archive aktivieren oder deaktivieren, sowie die maximale Größe der zu untersuchenden Archive begrenzen.

Wenn Ihr Computer nicht durch die Mittel eines lokalen Netzwerks geschützt ist (die Internetverbindung erfolgt ohne Proxyserver oder Firewall), wird davor gewarnt, die Untersuchung angehängter Archive zu deaktivieren.

Gehen Sie folgendermaßen vor, um die Untersuchungsparameter für zusammengesetzte Dateien anzupassen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Mail-Anti-Virus**.
4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
5. Geben Sie im folgenden Fenster auf der Registerkarte **Allgemein** die entsprechenden Parameter an.

E-MAIL-UNTERSUCHUNG IN MICROSOFT OFFICE OUTLOOK

Wenn Microsoft Office Outlook als Mailprogramm verwendet wird, können Sie die Einstellungen für die Virenuntersuchung Ihrer E-Mails zusätzlich anpassen.

Bei der Installation von Kaspersky PURE wird ein spezielles Erweiterungsmodul in Microsoft Office Outlook integriert. Es erlaubt Ihnen, schnell zu den Einstellungen von Mail-Anti-Virus zu wechseln und festzulegen, wann eine E-Mail-Nachricht auf das Vorhandensein gefährlicher Objekte untersucht werden soll.

Das Erweiterungsmodul besitzt die Form einer Registerkarte mit dem Namen **E-Mail-Schutz**, die sich im Menü **Extras** → **Optionen** befindet.

Gehen Sie folgendermaßen vor, um zu wählen, wann die Untersuchung von E-Mails erfolgen soll:

1. Öffnen Sie das Hauptfenster von Microsoft Office Outlook.
2. Wählen Sie im Programmmenü den Punkt **Extras** → **Optionen**.
3. Wählen Sie auf der Registerkarte **E-Mail-Schutz** die erforderlichen Parameter.

E-MAIL-UNTERSUCHUNG IN THE BAT!

Die Aktionen für infizierte E-Mail-Objekte werden im Mailprogramm The Bat! durch Mittel des Programms festgelegt.

Die Parameter von Mail-Anti-Virus, die festlegen, ob ein- und ausgehende E-Mails untersucht werden oder nicht, und die Aktionen für gefährliche E-Mail-Objekte und Ausnahmen bestimmen, werden ignoriert. Das Programm The Bat! berücksichtigt lediglich die Untersuchung angehängter Archive.

Die Parameter für den E-Mail-Schutz gelten für alle auf dem Computer installierten Antiviren-Komponenten, die die Arbeit mit The Bat! unterstützen.

Es sollte beachtet werden, dass E-Mails beim Empfang zuerst von Mail-Anti-Virus untersucht werden und erst anschließend von dem Plug-in des Mailprogramms The Bat!. Wenn ein schädliches Objekt gefunden wird, werden Sie von Kaspersky PURE auf jeden Fall darüber informiert. Wenn dabei im Meldungsfenster von Mail-Anti-Virus die Aktion **Desinfizieren** (**Löschen**) gewählt wird, führt Mail-Anti-Virus das Löschen der Bedrohung aus. Wird im Meldungsfenster die Aktion **Überspringen** gewählt, so wird das Objekt von dem Plug-in für The Bat! desinfiziert. Beim Senden werden E-Mails zuerst von dem Plug-in und anschließend von Mail-Anti-Virus untersucht.

Legen Sie folgende Kriterien fest:

- Welche Richtung des E-Mail-Verkehrs (eingehend, ausgehend) der Virenuntersuchung unterzogen werden soll.
- Wann die Untersuchung von Mail-Objekten erfolgen soll (beim Öffnen einer Mail oder vor dem Speichern auf der Festplatte).
- Welche Aktionen das Mailprogramm ausführen soll, wenn gefährliche Objekte gefunden werden. Es stehen beispielsweise zur Auswahl:
  - **Reparaturversuch infizierter Teile** – Bei Auswahl dieser Variante wird versucht, ein infiziertes Objekt zu desinfizieren. Wenn die Desinfektion fehlschlägt, verbleibt das Objekt in der Nachricht.
  - **Infizierte Teile löschen** – Bei Auswahl dieser Variante wird ein gefährliches E-Mail-Objekt gelöscht. Dabei bleibt unberücksichtigt, ob es infiziert ist oder als verdächtig gilt.

Standardmäßig verschiebt das Programm The Bat! alle infizierten E-Mail-Objekte ohne Desinfektion in die Quarantäne.

E-Mail-Nachrichten, die gefährliche Objekte enthalten, werden von dem Programm The Bat! nicht durch eine spezielle Kopfzeile gekennzeichnet.

Gehen Sie folgendermaßen vor, um in The Bat! die Einstellungen für den E-Mail-Schutz anzupassen:

1. Öffnen Sie das Hauptfenster von The Bat!.
2. Wählen Sie im Menü **Optionen** des Mailprogramms den Punkt **Benutzereinstellungen**.
3. Wählen Sie in der Konfigurationsstruktur das Objekt **Virenschutz**.

WEB-ANTI-VIRUS

Bei der Arbeit im Internet besteht für die Informationen, die auf Ihrem Computer gespeichert sind, ständig das Risiko einer Infektion durch gefährliche Programme. Sie können in Ihren Computer eindringen, während Sie kostenlose Programme herunterladen oder scheinbar ungefährliche Webseiten besuchen (die zuvor von Hackern angegriffen wurden). Außerdem können Netzwürmer direkt beim Aufbau einer Internetverbindung in Ihren Computer eindringen, bevor überhaupt eine Webseite geöffnet oder eine Datei heruntergeladen wird.

Die Sicherheit Ihrer Arbeit im Internet wird von der Komponente *Web-Anti-Virus* gewährleistet. Er schützt Informationen, die über die Protokolle HTTP, HTTPS und FTP auf Ihren Computer gelangen, und verhindert auf Ihrem Computer den Start gefährlicher Skripts.

Der Web-Schutz sieht nur die Kontrolle des Datenstroms vor, der über die Ports übertragen wird, die auf der Liste der kontrollierten Ports stehen. Eine Liste der Ports, die am häufigsten zur Datenübertragung dienen, ist im Lieferumfang von Kaspersky PURE enthalten. Wenn Sie Ports verwenden, die nicht zu dieser Liste gehören, fügen Sie diese zur Liste der kontrollierten Ports hinzu (s. Abschnitt "Liste der zu kontrollierenden Ports erstellen" auf S. 160), um den Schutz des über sie abgewickelten Datenverkehrs sicherzustellen.

Die Untersuchung des Datenstroms erfolgt mit einer bestimmten Auswahl von Parametern, die als Sicherheitsstufe bezeichnet wird (s. Abschnitt "Sicherheitsstufe ändern und wiederherstellen" auf S. 113). Beim Fund von Bedrohungen führt Web-Anti-Virus die festgelegte Aktion.

Die Spezialisten von Kaspersky Lab warnen davor, die Funktionsparameter von Web-Anti-Virus zu verändern. In den meisten Fällen ist es ausreichend, eine passende Sicherheitsstufe zu wählen.

Algorithmus für die Arbeit der Komponente

Web-Anti-Virus schützt Informationen, die über das HTTP-, HTTPS- und FTP-Protokoll auf Ihren Computer gelangen oder von ihm gesendet werden, und verhindert auf Ihrem Computer den Start gefährlicher Skripts. Die Untersuchung geschützter Verbindungen (nach HTTPS-Protokoll) ist standardmäßig deaktiviert. Sie kann aktiviert und angepasst werden (s. Abschnitt "Untersuchung geschützter Verbindungen" auf S. 157).

Der Schutz der Daten erfolgt nach folgendem Algorithmus:

1. Jede Webseite oder Datei, auf die ein Benutzer oder ein bestimmtes Programm über die Protokolle HTTP, HTTPS oder FTP zugreift, wird von Web-Anti-Virus abgefangen und auf schädlichen Code analysiert. Die Suche nach schädlichen Objekten erfolgt auf Basis der Datenbanken, die bei der Arbeit von Kaspersky PURE verwendet werden, sowie mit Hilfe eines heuristischen Algorithmus. Die Datenbanken enthalten eine Beschreibung aller momentan bekannten schädlichen Programme und entsprechende Desinfektionsmethoden. Der heuristische Algorithmus erlaubt es, neue Viren zu erkennen, die noch nicht in den Datenbanken beschrieben sind.

2. Aufgrund der Virenuntersuchung bestehen folgende Varianten für das weitere Vorgehen:

   - Wenn eine Webseite oder ein Objekt, auf das ein Benutzer zugreift, schädlichen Code enthält, wird der Zugriff darauf blockiert. Dabei erscheint auf dem Bildschirm eine Meldung darüber, dass das angeforderte Objekt oder die Seite infiziert ist.

   - Wenn die Datei oder Webseite keinen schädlichen Code enthält, erhält der Benutzer sofort Zugriff darauf.

Die Untersuchung von Skripts wird nach folgendem Algorithmus ausgeführt:

1. Jedes auszuführende Skript wird von Web-Anti-Virus abgefangen und auf schädlichen Code analysiert.

2. Wenn ein Skript schädlichen Code enthält, wird es von Web-Anti-Virus gesperrt und der Benutzer wird durch eine spezielle Bildschirmmeldung darüber informiert.

3. Wenn im Skript kein schädlicher Code gefunden wird, wird es ausgeführt.

Web-Anti-Virus fängt nur Skripts ab, die auf der Technologie Microsoft Windows Script Host basieren.

IN DIESEM ABSCHNITT

Web-Anti-Virus aktivieren und deaktivieren 113

Sicherheitsstufe ändern und wiederherstellen 113

Aktion für gefundene Objekte ändern 114

Gefährliche Skripts blockieren 114

Link-Untersuchung mit den Datenbanken für verdächtige und Phishing-Adressen 114

Heuristische Analyse verwenden 115

Untersuchung optimieren 115

Modul zur Link-Untersuchung 116

Liste mit vertrauenswürdigen Adressen erstellen 117

WEB-ANTI-VIRUS AKTIVIEREN UND DEAKTIVIEREN

Web-Anti-Virus ist standardmäßig aktiviert und arbeitet im optimalen Modus. Bei Bedarf kann Web-Anti-Virus deaktiviert werden.

Gehen Sie folgendermaßen vor, um Web-Anti-Virus zu aktivieren oder zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.
4. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Web-Anti-Virus aktivieren**, um die Komponente auszuschalten. Aktivieren Sie dieses Kontrollkästchen, um die Komponente einzuschalten.

SICHERHEITSSTUFE ÄNDERN UND WIEDERHERSTELLEN

Abhängig von den aktuellen Erfordernissen können Sie eine vordefinierte Sicherheitsstufe auswählen oder die Einstellungen für Web-Anti-Virus entsprechend anpassen.

Während der Konfiguration einer Komponente können Sie jederzeit zu den empfohlenen Einstellungen zurückkehren. Diese Werte gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und entsprechen der Sicherheitsstufe **Empfohlen**.

Gehen Sie folgendermaßen vor, um die festgelegte Sicherheitsstufe für den Web-Datenverkehr zu ändern:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.
4. Stellen Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** die erforderliche Sicherheitsstufe ein oder klicken Sie auf **Einstellungen**, um die Untersuchungseinstellungen manuell anzupassen.

Wenn manuelle Änderungen erfolgen, ändert sich der Name der Sicherheitsstufe in **Benutzerdefiniert**.

Gehen Sie folgendermaßen vor, um die standardmäßigen Einstellungen für den Schutz des Web-Datenverkehrs wiederherzustellen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.
4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Standard**.

AKTION FÜR GEFUNDENE OBJEKTE ÄNDERN

Beim Fund infizierter oder möglicherweise infizierter Objekte führt das Programm eine Aktion aus. Das Vorgehen ist davon abhängig, ob der automatische oder interaktive Modus ausgewählt wurde.

Wenn Sie im automatischen Modus (s. Abschnitt "Interaktiven Schutzmodus verwenden" auf S. 61), wendet Kaspersky PURE beim Fund gefährlicher Objekte automatisch die von Kaspersky Lab empfohlene Aktion an. Für schädliche Objekte ist dies die Aktion **Desinfizieren. Löschen, wenn Desinfektion nicht möglich**, für verdächtige – **In die Quarantäne verschieben**. Wenn Sie im interaktiven Modus arbeiten (s. Abschnitt "Interaktiven Schutzmodus verwenden" auf S. 61), zeigt das Programm beim Fund gefährlicher Objekte auf dem Bildschirm eine Meldung an, in der Sie eine Aktion auswählen können.

Gehen Sie folgendermaßen vor, um die festgelegte Aktion für gefundene Objekte zu ändern:

1. Öffnen Sie das Programmhauptfenster das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.
4. Wählen Sie auf der rechten Fensterseite im Block **Aktion** die entsprechende Variante.

GEFÄHRLICHE SKRIPTS BLOCKIEREN

Web-Anti-Virus kann alle Skripts, die in Microsoft Internet Explorer verarbeitet werden, und alle WSH-Skripts (JavaScript, Visual Basic Script u.a.), die bei der Arbeit eines Benutzers auf dem Computer gestartet werden, untersuchen. Wenn ein Skript den Computer gefährden kann, wird seine Ausführung blockiert.

Gehen Sie folgendermaßen vor, damit Web-Anti-Virus Skripts untersucht und blockiert:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.
4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
5. Im folgenden Fenster **Web-Anti-Virus** muss im Block **Erweitert** das Kontrollkästchen **Gefährliche Skripts in Microsoft Internet Explorer blockieren** aktiviert sein. Wenn dieses Kontrollkästchen nicht angekreuzt ist, aktivieren Sie es.

LINK-UNTERSUCHUNG MIT DEN DATENBANKEN FÜR VERDÄCHTIGE UND PHISHING-ADRESSEN

Web-Anti-Virus untersucht den Web-Datenverkehr auf Viren und stellt fest, ob Links auf der Liste für verdächtige Webadressen oder auf der Liste für Phishing-Webadressen stehen.

Durch die Untersuchung von Links auf die Zugehörigkeit zur Liste der Phishing-Adressen lassen sich Phishing-Angriffe abwehren, die in der Regel die Form von E-Mails besitzen, die scheinbar von finanziellen Strukturen stammen und Links auf deren Webseiten enthalten. Die Nachricht fordert dazu auf, einem Link zu folgen und auf der betreffenden Webseite vertrauliche Informationen wie beispielsweise eine Kreditkartennummer oder Benutzername und Kennwort für die persönliche Online-Banking-Seite einzugeben, auf der finanzielle Operationen erfolgen können. Ein häufiges Beispiel für Phishing-Angriffe ist ein Brief, der scheinbar von einer Bank stammt, bei der Sie Kunde sind, und einen Link zu der offiziellen Webseite der Bank enthält. Wenn Sie dem Link folgen, gelangen Sie auf eine Webseite, die eine genaue Kopie der Bankseite darstellt und im Browser sogar deren Adresse anzeigen kann, obwohl Sie sich in Wirklichkeit auf einer fiktiven Webseite befinden. Alle Aktionen, die Sie auf dieser Webseite ausführen, werden verfolgt und können zum Diebstahl Ihres Geldes missbraucht werden.

Listen mit Phishing-Webadressen gehören zum Lieferumfang von Kaspersky PURE. Da sich ein Phishing-Link nicht nur in E-Mails, sondern beispielsweise auch im Text einer ICQ-Nachricht befinden kann, überwacht Web-Anti-Virus alle Versuche zum Öffnen einer Phishing-Seite auf der Ebene des Web-Datenverkehrs und blockiert den Zugriff auf solche Webseiten.

- *Gehen Sie folgendermaßen vor, damit Web-Anti-Virus alle Links mit den Datenbanken für verdächtige und Phishing-Webadressen untersucht:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.
4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
5. Im folgenden Fenster **Web-Anti-Virus** müssen im Block **Untersuchungsmethoden** die Kontrollkästchen **Links mit der Datenbank für verdächtige Webadressen untersuchen** und **Links mit der Datenbank für Phishing-Webadressen untersuchen** aktiviert ist. Wenn die Kontrollkästchen nicht angekreuzt sind, aktivieren Sie sie.

HEURISTISCHE ANALYSE VERWENDEN

Bei der Arbeit von Mail-Anti-Virus wird immer die Methode *Signaturanalyse* verwendet, bei der Kaspersky PURE ein gefundenes Objekt mit den Einträgen in den Datenbanken vergleicht.

Um die Effektivität des Schutzes zu steigern, können Sie eine *heuristische Analyse* verwenden (Analyse der Aktivität, die ein Objekt im System zeigt). Diese Analyse erlaubt die Erkennung neuer Schadobjekte, über die noch keine Datenbankeinträge vorliegen.

- *Gehen Sie folgendermaßen vor, um die Verwendung der heuristischen Analyse zu aktivieren oder zu deaktivieren:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.
4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
5. Aktivieren Sie im folgenden Fenster **Web-Anti-Virus** im Block **Untersuchungsmethoden** das Kontrollkästchen **Heuristische Analyse** und stellen Sie darunter die Genauigkeitsstufe der Untersuchung ein. Deaktivieren Sie das Kontrollkästchen **Heuristische Analyse**, wenn diese Untersuchungsmethode nicht verwendet werden soll.

UNTERSUCHUNG OPTIMIEREN

Um die Effektivität der Erkennung von schädlichem Code durch Web-Anti-Virus zu steigern, wird für Objekte, die aus dem Internet heruntergeladen werden, die Zwischenspeicherung von Fragmenten verwendet. Allerdings erhöht sich durch die Cache-Verwendung die Untersuchungsdauer und es können Probleme beim Kopieren und bei der Bearbeitung großer Objekte auftreten. Um die Arbeit mit Objekten, die aus dem Internet heruntergeladen werden, zu optimieren, können Sie die Dauer der Zwischenspeicherung von Objektfragmenten beschränken.

Gehen Sie folgendermaßen vor, um die Dauer der Zwischenspeicherung zu beschränken:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.
4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
5. Aktivieren Sie im folgenden Fenster **Web-Anti-Virus** im Block **Untersuchung optimieren** das Kontrollkästchen **Zwischenspeicherung des Datenverkehrs maximal** und geben Sie im Feld rechts den Zeitraum (in Sekunden) an.

MODUL ZUR LINK-UNTERSUCHUNG

Kaspersky PURE umfasst ein Modul zur Link-Untersuchung, das zu der Komponente Web-Anti-Virus gehört. Das Modul wird als Plug-in in die Webbrowser Microsoft Internet Explorer und Mozilla Firefox integriert.

Das Modul untersucht alle Links, die auf einer Webseite vorhanden sind, auf Zugehörigkeit zu verdächtigen und Phishing-Webadressen. Sie können folgende Listen anlegen: eine Liste mit Webseiten, deren Inhalt nicht auf verdächtige und Phishing-Links untersucht werden soll, oder eine Liste mit Webseiten, deren Inhalt untersucht werden soll. Sie können die Link-Untersuchung auch ganz ausschalten.

Gehen Sie folgendermaßen vor, um das Modul zur Link-Untersuchung zu aktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.
4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
5. Aktivieren Sie im folgenden Fenster **Web-Anti-Virus** im Block **Erweitert** das Kontrollkästchen **Phishing-Links und verdächtige Links im Microsoft Internet Explorer und Mozilla Firefox kennzeichnen**.

Gehen Sie folgendermaßen vor, um eine Liste der Webadressen anzulegen, deren Inhalt nicht auf verdächtige und Phishing-Links untersucht werden soll:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.
4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
5. Klicken Sie im folgenden Fenster **Web-Anti-Virus** im Block **Erweitert** auf **Einstellungen**.
6. Wählen Sie im folgenden Fenster **Modul zur Link-Untersuchung** die Variante **Für alle Webadressen** und klicken Sie auf **Ausnahmen**.
7. Legen Sie im folgenden Fenster **Vertrauenswürdige Webadressen** eine Liste der Webadressen an, deren Inhalt nicht auf verdächtige Links und Phishing-Links untersucht werden soll.

Gehen Sie folgendermaßen vor, um eine Liste der Webadressen anzulegen, deren Inhalt auf verdächtige und Phishing-Links untersucht werden soll:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.

4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.

5. Klicken Sie im folgenden Fenster **Web-Anti-Virus** im Block **Erweitert** auf **Einstellungen**.

6. Wählen Sie im folgenden Fenster **Modul zur Link-Untersuchung** die Variante **Für die angegebenen Webadressen** und klicken Sie auf **Auswählen**.

7. Legen Sie im folgenden Fenster **Liste der zu untersuchenden Webadressen** eine Liste der Webadressen an, deren Inhalt auf verdächtige und Phishing-Links untersucht werden soll.

LISTE MIT VERTRAUENSWÜRDIGEN ADRESSEN ERSTELLEN

Sie können eine Liste der Webadressen anlegen, deren Inhalt Sie vorbehaltlos vertrauen. Web-Anti-Virus wird die Informationen von diesen Adressen nicht auf gefährliche Objekte hin analysieren. Diese Option kann beispielsweise verwendet werden, wenn Web-Anti-Virus den Download einer bestimmten Datei von einer Ihnen bekannten Webseite verhindert.

Gehen Sie folgendermaßen vor, um eine Liste mit vertrauenswürdigen Adressen anzulegen:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.

4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.

5. Aktivieren Sie im folgenden Fenster **Web-Anti-Virus** im Block **Untersuchung optimieren** das Kontrollkästchen **HTTP-Datenverkehr von vertrauenswürdigen Webadressen nicht untersuchen** und klicken Sie auf **Auswählen**.

6. Erstellen Sie im folgenden Fenster **Liste der vertrauenswürdigen Webadressen** eine Liste der Adressen, deren Inhalt Sie vertrauen.

Um eine Adresse vorübergehend aus der vertrauenswürdigen Liste auszuschließen, ohne sie aus der Liste zu löschen, deaktivieren Sie das entsprechende Kontrollkästchen .

IM-ANTI-VIRUS

IM-Anti-Virus untersucht den Datenverkehr, der mit Programmen zum Sofortaustausch von Nachrichten (so genannte *Instant Messenger*) übertragen wird.

Nachrichten, die mit Instant Messengern übertragen werden, können Links zu Webseiten enthalten, die verdächtig sind oder die von Angreifern für Phishing-Angriffe verwendet werden. Schädliche Programme verwenden Instant-Messenger zum Senden von Spam-Nachrichten. Außerdem können Sofortnachrichten Links zu Programmen (oder sogar Programme) enthalten, die Nummern und Kennwörter der Benutzer stehlen.

Kaspersky PURE gewährleistet Sicherheit bei der Arbeit mit einer Vielzahl von Programmen, die dem Sofortaustausch von Nachrichten dienen. Dazu zählen ICQ, MSN, AIM, Yahoo! Messenger, Jabber, Google Talk, Mail.Ru Agent und IRC.

Manche Instant Messenger wie z.B. Yahoo! Messenger und Google Talk verwenden eine geschützte Verbindung. Um den Datenverkehr dieser Programme zu untersuchen, muss die Untersuchung von geschützten Verbindungen aktiviert werden (s. S. 157).

Die Nachrichten werden von IM-Anti-Virus abgefangen und auf gefährliche Objekte und Links geprüft. Sie können die Nachrichtentypen (s. S. 118) wählen, die untersucht werden sollen, und unterschiedliche Untersuchungsmethoden einsetzen.

Wenn IM-Anti-Virus in einer Nachricht eine Bedrohung findet, wird die Nachricht durch eine Warnung für den Benutzer ersetzt.

Dateien, die über einen Instant-Messenger übertragen werden, werden von der Komponente Datei-Anti-Virus (s. S. 99) untersucht, wenn versucht wird sie zu speichern.

IN DIESEM ABSCHNITT

IM-Anti-Virus aktivieren und deaktivieren 118

Schutzbereich festlegen 118

Untersuchungsmethode auswählen 118

IM-ANTI-VIRUS AKTIVIEREN UND DEAKTIVIEREN

IM-Anti-Virus ist standardmäßig aktiviert und arbeitet im optimalen Modus. Bei Bedarf kann IM-Anti-Virus deaktiviert werden.

Gehen Sie folgendermaßen vor, um IM-Anti-Virus zu aktivieren oder zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **IM-Anti-Virus**.
4. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **IM-Anti-Virus aktivieren**, um die Komponente auszuschalten. Aktivieren Sie dieses Kontrollkästchen, um die Komponente einzuschalten.

SCHUTZBEREICH FESTLEGEN

Unter Schutzbereich wird der Typ der Nachrichten verstanden, die untersucht werden sollen. Standardmäßig untersucht Kaspersky PURE sowohl eingehende, als auch ausgehende E-Mails. Wenn Sie sicher sind, dass die von Ihnen gesendeten Nachrichten keine gefährlichen Objekte enthalten, können Sie die Untersuchung des ausgehenden Datenverkehrs deaktivieren.

Gehen Sie folgendermaßen vor, um die Untersuchung ausgehender Nachrichten zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **IM-Anti-Virus**.
4. Wählen Sie auf der rechten Fensterseite im Block **Schutzbereich** die Variante **Nur eingehende Nachrichten**.

UNTERSUCHUNGSMETHODE AUSWÄHLEN

Die Untersuchungsmethoden beziehen sich hier auf die Untersuchung der in Instant Messenger-Nachrichten enthaltenen Links auf ihre Zugehörigkeit zur Liste für verdächtige Adressen und (oder) zur Liste der Phishing-Adressen.

Um die Effektivität des Schutzes zu steigern, können Sie eine *heuristische Analyse* verwenden (Analyse der Aktivität, die ein Objekt im System zeigt). Diese Analyse erlaubt die Erkennung neuer Schadobjekte, über die noch keine Datenbankeinträge vorliegen. Bei der heuristischen Analyse werden alle Skripts, die in Instant Messenger-Nachrichten enthalten sind, in der einer geschützten Umgebung ausgeführt. Wenn die erkannte Aktivität eines Skripts als typisch für

schädliche Objekte gilt, lässt sich das Objekt mit hoher Wahrscheinlichkeit als schädlich oder verdächtig einstufen. In der Grundeinstellung ist die heuristische Analyse aktiviert.

Gehen Sie folgendermaßen vor, um die in E-Mails enthaltenen Links mit der Datenbank für verdächtige Adressen zu untersuchen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **IM-Anti-Virus**.
4. Aktivieren Sie auf der rechten Fensterseite im Block **Untersuchungsmethoden** das Kontrollkästchen **Links mit der Datenbank für verdächtige Webadressen untersuchen**.

Gehen Sie folgendermaßen vor, um die in E-Mails enthaltenen Links mit der Datenbank für verdächtige Adressen zu untersuchen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **IM-Anti-Virus**.
4. Aktivieren Sie auf der rechten Fensterseite im Block **Untersuchungsmethoden** das Kontrollkästchen **Links mit der Datenbank für Phishing-Webadressen untersuchen**.

Gehen Sie folgendermaßen vor, um die Verwendung der heuristischen Analyse zu aktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **IM-Anti-Virus**.
4. Aktivieren Sie auf der rechten Fensterseite im Block **Untersuchungsmethoden** das Kontrollkästchen **Heuristische Analyse** und stellen Sie darunter das Genauigkeitsniveau ein.

ANTI-SPAM

Anti-Spam ist eine spezielle Komponente von Kaspersky PURE, die unerwünschte E-Mails (Spam) erkennt und sie nach den Regeln Ihres Mailprogramms verarbeitet. Mit dieser Komponente lässt sich bei der Arbeit mit E-Mails Zeit sparen.

Anti-Spam wird als Erweiterungsmodul in folgende Mailprogramme integriert:

- Microsoft Office Outlook (auf S. 134).
- Microsoft Outlook Express (Windows Mail) (auf S. 134).
- The Bat! (auf S. 135).
- Thunderbird (auf S. 135).

Legen Sie Listen für erlaubte und verbotene Absender an, um für Anti-Spam festzulegen, von welchen Adressen erwünschte E-Mails bzw. Spam-Mails zu erwarten sind. Als Spam können auch Nachrichten gelten, die nicht an Sie adressiert sind (s. S. 128). Außerdem kann Anti-Spam eine E-Mail auf das Vorhandensein von erlaubten und verbotenen Phrasen sowie von Phrasen aus der Liste für anstößige Ausdrücke analysieren.

Eine Voraussetzung für die effektive Unterscheidung zwischen Spam und nützlichen E-Mails, ist ein Training von Anti-Spam (s. Abschnitt "Anti-Spam-Training" auf S. 122).

Algorithmus für die Arbeit der Komponente

Anti-Spam verwendet einen lernfähigen Algorithmus, mit dem die Komponente mit der Zeit genauer zwischen Spam und nützlicher E-Mails unterscheiden kann. Als Datenquelle für den Algorithmus dient der Inhalt einer E-Mail.

Die Arbeit der Komponente Anti-Spam besteht aus zwei Etappen:

1. Anwendung von strengen Kriterien für die Filterung einer Nachricht.. Diese Kriterien ermöglichen es, schnell festzustellen, ob eine Nachricht Spam ist. Anti-Spam weist der Nachricht den Status *Spam* oder *Kein Spam*, die Untersuchung wird beendet und die Nachricht zur Bearbeitung an das Mailprogramm weitergeleitet (siehe unten: Schritte 1– 5).

2. Analyse von E-Mails, die nach den strengen Kriterien der vorhergehenden Schritte nicht eingestuft werden konnten. Solche Nachrichten lassen sich nicht eindeutig als Spam bewerten. Deshalb muss Anti-Spam die *Wahrscheinlichkeit* berechnen, mit der es sich bei einer Nachricht um Spam handelt.

Der Algorithmus für die Arbeit von Anti-Spam umfasst folgende Schritte:

1. Es wird geprüft, ob die Absenderadresse einer E-Mail auf den Listen für erlaubte und verbotene Absender steht.

   - Wenn die Absenderadresse in der Liste mit erlaubten Adressen steht, erhält die Nachricht den Status *Kein Spam*.

   - Wenn die Absenderadresse in der Liste mit verbotenen Adressen steht, erhält die Nachricht den Status *Spam*.

2. Wurde die Nachricht mit Hilfe von Microsoft Exchange Server gesendet und die Untersuchung solcher Nachrichten ist deaktiviert, dann erhält sie den Status *Kein Spam*.

3. Die Nachricht wird auf das Vorhandensein von Zeilen aus der Liste mit erlaubten Phrasen analysiert. Wenn mindestens eine Zeile aus dieser Liste gefunden wird, erhält die Nachricht den Status *Kein Spam*. Dieser Schritt wird standardmäßig übersprungen.

4. Es wird analysiert, ob die Nachricht Zeilen aus der Liste der verbotenen Phrasen und der Liste der anstößigen Phrasen enthält. Werden in einer Nachricht Wörter aus diesen Listen gefunden, so werden ihre gewichteten Koeffizienten summiert. Wenn die Summe der Koeffizienten über 100 liegt, erhält die Nachricht den Status *Spam*. Dieser Schritt wird standardmäßig übersprungen.

5. Wenn der Nachrichtentext eine Adresse enthält, die in der Datenbank von verdächtigen oder Phishing-Adressen steht, erhält die Nachricht den Status *Spam*.

6. Die Nachricht wird mit Hilfe heuristischer Regeln analysiert. Wenn aufgrund dieser Analyse in E-Mails typische Spam-Merkmale gefunden werden, erhöht sich die Wahrscheinlichkeit, dass es sich um Spam handelt.

7. Die Nachricht wird mit Hilfe der GSG-Technologie analysiert. Dabei überprüft Anti-Spam die in der E-Mail enthaltenen Bilder. Wenn in den Bildern typische Spam-Merkmale gefunden werden, erhöht sich die Wahrscheinlichkeit, dass es sich um Spam handelt.

8. Dokumente des Formats .rtf, die an eine E-Mail angehängt sind, werden analysiert. Anti-Spam sucht in angehängten Dokumenten nach typischen Spam-Merkmalen.. Zum Abschluss der Analyse berechnet Anti-Spam, wie stark sich die Wahrscheinlichkeit erhöht hat, dass es sich bei der Nachricht um Spam handelt. Diese Technologie ist standardmäßig deaktiviert.

9. Das Vorhandensein zusätzlicher Merkmale, die für Spam charakteristisch sind, wird überprüft. Jede Übereinstimmung erhöht die Wahrscheinlichkeit, dass es sich um Spam handelt.

10. Wenn mit Anti-Spam bereits ein Training ausgeführt wurde, wird die Nachricht mit Hilfe der iBayes-Technologie untersucht. Der lernfähige iBayes-Algorithmus berechnet die Wahrscheinlichkeit, mit der es sich bei der Nachricht um Spam handelt. Dazu wird analysiert, wie häufig im Text der Nachricht typische Spam-Phrasen vorkommen.

Die Nachrichtenanalyse ergibt eine Wahrscheinlichkeit, mit der die E-Mail als Spam gilt. Diese Wahrscheinlichkeit wird durch den Wert des *Spam-Faktors* angegeben. Abhängig von den Grenzwerten für den Spam-Faktor wird einer Nachricht der Status *Spam* oder *potentieller Spam* zugewiesen (s. Abschnitt "Grenzwerte für den Spam-Faktor

regulieren" auf S. 130). Außerdem wird für Spam und potentiellen Spam im Feld **Betreff** standardmäßig die Markierung **[!! SPAM]** oder **[!! Probable Spam]** (s. Abschnitt "**Markierung zum Betreff einer Nachricht hinzufügen**" auf S. 132) hinzugefügt. Anschließend wird die Nachricht nach den von Ihnen definierten Regeln für Mailprogramme (s. Abschnitt "Spam-Verarbeitung in Mailprogrammen anpassen" auf S. 133) verarbeitet.

IN DIESEM ABSCHNITT

Anti-Spam aktivieren und deaktivieren 121

Sicherheitsstufe ändern und wiederherstellen 121

Anti-Spam-Training 122

Links in Nachrichten untersuchen 125

Spam nach Phrasen und Adressen ermitteln. Listen erstellen 125

Grenzwerte für den Spam-Faktor regulieren 130

Zusätzliche Merkmale für die Spam-Filterung verwenden 131

Algorithmus zur Spam-Erkennung auswählen 131

Markierung zum Betreff einer Nachricht hinzufügen 132

Filterung von E-Mails auf dem Server. Mail-Manager 132

Nachrichten für Microsoft Exchange Server von der Untersuchung ausschließen 133

Spam-Verarbeitung in Mailprogrammen anpassen 133

ANTI-SPAM AKTIVIEREN UND DEAKTIVIEREN

Anti-Spam ist standardmäßig aktiviert und arbeitet im optimalen Modus. Bei Bedarf kann Anti-Spam deaktiviert werden.

Gehen Sie folgendermaßen vor, um Anti-Spam zu aktivieren oder zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
4. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Anti-Spam aktivieren**, um die Komponente auszuschalten. Aktivieren Sie dieses Kontrollkästchen, um die Komponente einzuschalten.

SICHERHEITSSTUFE ÄNDERN UND WIEDERHERSTELLEN

Abhängig von den aktuellen Erfordernissen können Sie eine vordefinierte Sicherheitsstufe auswählen oder die Einstellungen für Anti-Spam entsprechend anpassen.

Während der Konfiguration einer Komponente können Sie jederzeit zu den empfohlenen Einstellungen zurückkehren. Diese Werte gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und entsprechen der Sicherheitsstufe **Empfohlen**.

Gehen Sie folgendermaßen vor, um die festgelegte Sicherheitsstufe für Anti-Spam zu ändern:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
4. Stellen Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** die erforderliche Sicherheitsstufe ein oder klicken Sie auf **Einstellungen**, um die Untersuchungseinstellungen manuell anzupassen.

   Wenn manuelle Änderungen erfolgen, ändert sich der Name der Sicherheitsstufe in **Benutzerdefiniert**.

Gehen Sie folgendermaßen vor, um die standardmäßigen Einstellungen für Anti-Spam wiederherzustellen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Standard**.

ANTI-SPAM-TRAINING

Eines der Werkzeuge zur Spam-Erkennung ist der lernfähige iBayes-Algorithmus. Mit diesem Algorithmus wird auf Basis von Phrasen, die in einer Nachricht enthalten sind, darüber entschieden, welchen Status die Nachricht erhält. Bevor der iBayes-Algorithmus eingesetzt wird, benötigt Anti-Spam Zeilenmuster aus erwünschten und aus Spam-Mails. Dazu dient ein *Training.*

Es existieren mehrere Methoden für das Training von Anti-Spam:

- Verwendung eines Trainingsassistenten (Pakettraining). Das Training mit Hilfe des Trainingsassistenten sollte ganz zu Beginn der Arbeit mit Anti-Spam erfolgen.
- Anti-Spam-Training mit ausgehenden E-Mails.
- Training während der Arbeit mit E-Mails in einem Mailprogramm. Dazu dienen für das Training vorgesehene Schaltflächen und Menüpunkte.
- Training bei der Arbeit mit den Anti Spam-Berichten.

IN DIESEM ABSCHNITT

Trainingsassistent verwenden 122

Training mit ausgehenden E-Mails 123

Elemente der Benutzeroberfläche eines Mailprogramms verwenden 123

Adressen zur Liste der erlaubten Absender hinzufügen 124

Training mit Berichten 124

TRAININGSASSISTENT VERWENDEN

Der Trainingsassistent erlaubt es, ein Anti-Spam-Training im Paketmodus vorzunehmen. Dazu ist es erforderlich, die Ordner der Benutzerkonten für die Mailprogramme Microsoft Office Outlook und Microsoft Outlook Express (Windows Mail) anzugeben, in denen sich Spam bzw. erwünschte E-Mails befinden.

Für die korrekte Spam-Erkennung ist es erforderlich, ein Training mit mindestens 50 Mustern erwünschter Mails und 50 Spam-Mustern vorzunehmen. Der iBayes-Algorithmus funktioniert nur, wenn die genannten Aktionen ausgeführt wurden.

Um Zeit zu sparen, wird das Training mit dem Assistenten auf 50 Nachrichten aus jedem gewählten Ordner beschränkt.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**. Zum Abschluss des Assistenten dient die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf **Abbrechen** abgebrochen werden.

Gehen Sie folgendermaßen vor, den Assistenten zu starten:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
4. Klicken Sie auf der rechten Fensterseite im Block **Anti-Spam-Training** auf **Trainieren**.

Beim Training mit erwünschten Nachrichten werden die entsprechenden Absenderadressen automatisch zur Liste der erlaubten Absender hinzugefügt. Sie können diese Funktion deaktivieren (s. Abschnitt "Adressen zur Liste der erlaubten Absender hinzufügen" auf S. 124).

SIEHE AUCH

Wie mit einer großen Anzahl von Spam-Mails verfahren wird? 80

TRAINING MIT AUSGEHENDEN E-MAILS

Sie können Anti-Spam mit 50 ausgehenden E-Mails trainieren. Nachdem das Anti-Spam-Training aktiviert ist, wird jede von Ihnen gesendete Nachricht analysiert und als Muster für eine erwünschte Nachricht verwendet. Das Training wird abgeschlossen, nachdem 50 Nachrichten gesendet wurden.

Gehen Sie folgendermaßen vor, um das Anti-Spam-Training mit ausgehenden E-Mails zu aktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
5. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Ausgehende Mails** das Kontrollkästchen **Mit ausgehenden E-Mails trainieren**.

Beim Training mit ausgehenden Nachrichten werden die entsprechenden Empfängeradressen automatisch zur Liste der erlaubten Absender hinzugefügt. Sie können diese Funktion deaktivieren (s. Abschnitt "Adressen zur Liste der erlaubten Absender hinzufügen" auf S. 124).

ELEMENTE DER BENUTZEROBERFLÄCHE EINES MAILPROGRAMMS VERWENDEN

Das Training von Anti-Spam während der Arbeit mit der E-Mail-Korrespondenz erfolgt unter Verwendung spezieller Elemente auf der Benutzeroberfläche Ihres Mailprogramms.

Die Schaltflächen für das Anti-Spam-Training erscheinen auf der Programmoberfläche von Microsoft Office Outlook und Microsoft Outlook Express (Windows Mail), nachdem Kaspersky PURE installiert wurde.

Gehen Sie folgendermaßen vor, um Anti-Spam mit Hilfe eines Mailprogramms zu trainieren:

1. Starten Sie das Mailprogramm.
2. Wählen Sie eine Nachricht, mit deren Hilfe Sie Anti-Spam trainieren möchten.

3. Führen Sie - abhängig davon, welchen Mail-Client Sie verwenden - folgende Aktionen aus:

   - Klicken Sie in der Symbolleiste von Microsoft Office Outlook auf **Spam** oder **Kein Spam**.
   - Klicken Sie in der Symbolleiste von Microsoft Office Outlook (Windows Mail) auf **Spam** oder **Kein Spam**.
   - Verwenden Sie im Mailprogramm The Bat! die dafür vorgesehenen Punkte **Als Spam markieren** und **Als KEIN Spam markieren** im Menü **Extras**.
   - Verwenden Sie in der Symbolleiste von Mozilla Thunderbird die Schaltfläche **Spam/Kein Spam**.

Nachdem eine der oben genannten Aktionen ausgewählt wurde, führt Anti-Spam mit der ausgewählten Nachricht ein Training durch. Wenn Sie mehrere Nachrichten markieren, erfolgt das Training mit allen ausgewählten E-Mails.

Wenn eine Nachricht als nützlich markiert wird, wird die Absenderadresse zur Liste der erlaubten Absender hinzugefügt.

ADRESSEN ZUR LISTE DER ERLAUBTEN ABSENDER HINZUFÜGEN

Wenn Anti-Spam mit Hilfe des Trainingsassistenten an erwünschten Nachrichten oder direkt im Fenster des Mailprogramms trainiert wird, werden die Absenderadressen von erwünschten Mails automatisch zur Liste der erlaubten Absender (s. Abschnitt "Verbotene und erlaubte Absender" auf S. 128) hinzugefügt. Dieser Liste werden beim Training mit ausgehenden Nachrichten auch die Empfängeradressen der ausgehenden Mails hinzugefügt.

Sie können diese Funktion deaktivieren, damit die Trainingsergebnisse nicht automatisch zur Liste der erlaubten Absender hinzugefügt werden.

Gehen Sie folgendermaßen vor, damit Adressen nicht zur Liste für erlaubte Absender hinzugefügt werden:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
5. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Allgemein** im Block **Folgende Nachrichten als nützlich einstufen** das Kontrollkästchen **Von erlaubten Absendern** und klicken Sie auf **Auswählen**.

   Das Fenster **Erlaubte Absender** wird geöffnet.
6. Deaktivieren Sie das Kontrollkästchen **Beim Anti-Spam-Training im Mailprogramm Adressen von erlaubten Absendern hinzufügen**.

TRAINING MIT BERICHTEN

Es besteht die Möglichkeit, Anti-Spam auf Basis von Berichten zu trainieren. Solche Berichte enthalten Angaben über Nachrichten, die der Kategorie "potentieller Spam" angehören. Beim Training erhalten Nachrichten die Markierung **Spam** oder **Kein Spam**, und werden zu den Listen für erlaubte oder verbotene Absender hinzugefügt.

Gehen Sie folgendermaßen vor, um Anti-Spam an einem Bericht zu trainieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.

   Das Fenster **Computersicherheit** wird geöffnet.
2. Gehen Sie mit Hilfe des Links **Bericht** in das Berichtsfenster von Kaspersky PURE.
3. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf **Detaillierter Bericht**.

   Das Fenster **Detaillierter Bericht** wird geöffnet.
4. Wählen Sie links oben in der Dropdown-Liste die Komponente **Anti-Spam** aus.

5. Legen Sie auf der rechten Fensterseite aufgrund der Einträge in der Spalte **Objekt** die Mails fest, an denen Sie Anti-Spam trainieren möchten. Öffnen Sie für jede dieser Nachrichten das Kontextmenü (durch Rechtsklick) und wählen Sie eine entsprechende Aktion für die Nachricht:

   - Als Spam markieren
   - Als Kein Spam markieren
   - Zur Liste der erlaubten Absender hinzufügen
   - Zur Liste der erlaubten Absender hinzufügen

LINKS IN NACHRICHTEN UNTERSUCHEN

Anti-Spam kann prüfen, ob die in E-Mails enthaltenen Links auf der Liste verdächtiger Webadressen oder auf der Liste für Phishing-Webadressen stehen. Diese Listen gehören zum Lieferumfang von Kaspersky PURE. Wenn ein Phishing-Link oder ein verdächtiger Link in einer Nachricht oder Phishing-Elemente im Nachrichtentext gefunden werden, wird die Nachricht als Spam eingestuft.

Gehen Sie folgendermaßen vor, um die Link-Untersuchung mit den Datenbanken für verdächtige und Phishing-Adressen zu aktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
5. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Allgemein** im Block **Folgende Nachrichten als Spam einstufen** die Kontrollkästchen **Mit Links aus der Datenbank für verdächtige Webadressen** und **Mit Phishing-Elementen**.

SPAM NACH PHRASEN UND ADRESSEN ERMITTELN. LISTEN ERSTELLEN

Sie können folgende Listen erstellen: Listen für erlaubte, verbotene und anstößige Schlüsselphrasen, Listen für erlaubte und verbotene Absenderadressen, Liste für Ihre eigenen Adressen. Beim Einsatz dieser Listen untersucht Anti-Spam den Nachrichteninhalt auf das Vorkommen von Wortverbindungen, die auf der Phrasenliste stehen, und die Absender- und Empfängeradressen auf Übereinstimmungen mit den Einträgen in den Adressenlisten. Wenn eine entsprechende Phrase oder Adresse gefunden wird, identifiziert Anti-Spam die Nachricht - abhängig davon, auf welcher Liste die gefundene Phrase oder Adresse steht - als erwünscht oder als Spam.

Als Spam gelten Nachrichten:

- die verbotene oder anstößige Phrasen mit einem summierten gewichteten Koeffizienten von über 100 enthalten.
- die von einer verbotenen Adresse stammen oder nicht an Sie adressiert sind.

Als erwünscht gelten Nachrichten:

- die erlaubte Phrasen enthalten.
- die von einer erlaubten Adresse stammen.

Masken für Schlüsselphrasen und Absenderadressen

In den Listen für erlaubte, verbotene und anstößige Phrasen können *Masken für Phrasen* verwendet werden. In den Listen für erlaubte und verbotene Absenderadressen sowie in der Liste der vertrauenswürdigen Adressen können *Adressmasken* verwendet werden.

Eine *Maske* ist eine bestimmte Zeile, mit der eine Phrase oder Adresse verglichen wird. Bestimmte Zeichen werden in einer Maske als Platzhalter für andere Zeichen eingesetzt: ***** steht für eine beliebige Zeichenfolge und **?** für ein beliebiges Einzelzeichen. Wenn solche Zeichen in einer Maske verwendet werden, können mehrere Phrasen oder Adressen mit der Maske übereinstimmen (s. folgende Beispiele).

Wenn das Zeichen ***** oder **?** in einer Phrase enthalten ist (z.B. *Wie spät ist es?*), muss ihm das Zeichen **** vorangestellt werden, damit es von Anti-Spam korrekt interpretiert wird. Anstelle des Zeichens ***** muss in der Maske also die Verbindung ***** verwendet werden und anstelle von **?** die Verbindung **\?** (z.B. *Wie spät ist es*\?).

Beispiele für Phrasenmasken:

- *Besuchen Sie unser* * – dieser Maske entspricht eine Nachricht, die mit den Worten *Besuchen Sie unser* beginnt und beliebig fortgeführt wird

Beispiele für Adressenmasken:

- *admin@test.com* – Dieser Maske entspricht nur die Adresse *admin@test.com*.
- *admin@** – Dieser Maske entspricht die Adresse eines Absenders mit dem Namen *admin*, z.B. *admin@test.com*, *admin@example.org.*
- **@test** – Dieser Maske entspricht die Adresse eines beliebigen Absenders mit der Mail-Domain *test*, z.B. *admin@test.com*, *info@test.org.*
- *info.*@test.???* – dieser Maske entspricht die Adresse eines beliebigen Absenders einer Nachricht, dessen Name mit *info.* beginnt und dessen Maildomäne mit *test.* anfängt, woraufhin drei beliebige Zeichen folgen, z.B.: *info.product@test.com* oder *info.company@test.org*, nicht jedoch *info.product@test.ru*.

IN DIESEM ABSCHNITT

Verbotene und erlaubte Phrasen 126

Anstößige Phrasen 127

Verbotene und erlaubte Absender 128

Ihre Adressen 128

Phrasen und Adressen exportieren und importieren 129

VERBOTENE UND ERLAUBTE PHRASEN

In der Liste der *verbotenen Phrasen* können Sie Phrasen eintragen, die nach Ihrer Einschätzung für Spam charakteristisch sind, und für jede Phrase einen gewichteten Koeffizienten festlegen. Mit dem *gewichteten Koeffizienten* lässt sich angeben, wie charakteristisch eine Phrase für Spam-Nachrichten ist: Je höher der Koeffizient, desto wahrscheinlicher ist es, dass es sich bei einer Nachricht mit dieser Phrase um Spam handelt. Der gewichtete Koeffizient einer Phrase kann zwischen 0 und 100 liegen. Wenn die Summe der gewichteten Koeffizienten aller in einer Nachricht gefunden Phrasen über 100 liegt, wird die Nachricht als Spam betrachtet.

Schlüsselphrasen, die für erwünschte Nachrichten charakteristisch sind, können in die Liste für *erlaubte Phrasen* aufgenommen werden. Wenn eine solche Phrase in einer Nachricht gefunden wird, identifiziert Anti-Spam diese als erwünscht (Kein Spam).

In die Listen für verbotene und erlaubte Phrasen können vollständige Adressen und entsprechende Masken eingetragen werden (s. Abschnitt "Spam nach Phrasen und Adressen ermitteln. Listen erstellen" auf S. 125).

Gehen Sie folgendermaßen vor, um eine Liste mit verbotenen oder erlaubten Absendern zu erstellen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.

4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.

5. Führen Sie im nächsten Fenster auf der Registerkarte **Allgemein** folgende Aktionen aus:

   - Wenn eine Liste für verbotene Phrasen erstellt werden soll, aktivieren Sie im Block **Folgende Nachrichten als Spam einstufen** das Kontrollkästchen **Mit verbotenen Phrasen** und klicken Sie rechts auf **Auswählen**.

     Das Fenster **Liste mit verbotenen Phrasen** wird geöffnet.

   - Wenn eine Liste für erlaubte Phrasen erstellt werden soll, aktivieren Sie im Block **Folgende Nachrichten als erwünscht einstufen** das Kontrollkästchen **Mit erlaubten Phrasen** und klicken Sie rechts auf **Auswählen**.

     Das Fenster **Liste mit erlaubten Phrasen** wird geöffnet.

6. Öffnen Sie mit dem Link **Hinzufügen** das Fenster **Verbotene Phrase** (oder das Fenster **Erlaubte Phrase**).

7. Geben Sie eine vollständige Phrase oder eine entsprechende Maske ein, legen Sie einen gewichteten Koeffizienten für die verbotene Phrase fest und klicken Sie anschließend auf **OK**.

Damit eine bestimmte Maske nicht mehr verwendet wird, muss sie nicht gelöscht werden. Es ist ausreichend, im Fenster mit der Liste das entsprechende Kontrollkästchen zu deaktivieren.

ANSTÖßIGE PHRASEN

Im Lieferumfang von Kaspersky PURE befindet sich eine Liste mit anstößigen Phrasen, die Spezialisten von Kaspersky Lab erstellt haben. Die Liste enthält anstößige Phrasen, deren Vorhandensein in einer Nachricht mit großer Wahrscheinlichkeit darauf hinweist, dass es sich um Spam handelt. In diese Listen können vollständige Phrasen und entsprechende Masken eingetragen werden (s. Abschnitt "Spam nach Phrasen und Adressen ermitteln. Listen erstellen" auf S. 125).

Gehen Sie folgendermaßen vor, um die Liste der anstößigen Phrasen zu bearbeiten:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.

4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.

5. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Allgemein** im Block **Folgende Nachrichten als Spam einstufen** das Kontrollkästchen **Mit verbotenen Phrasen** und klicken Sie auf **Auswählen**.

   Das Fenster **Liste mit verbotenen Phrasen** wird geöffnet.

6. Aktivieren Sie das Kontrollkästchen **Anstößige Phrasen als verboten einstufen** und öffnen Sie mit dem Link **anstößige Phrasen** das Fenster **Vereinbarung**.

7. Lesen Sie den Vereinbarungstext. Wenn Sie den genannten Bedingungen zustimmen, aktivieren Sie unten das Kontrollkästchen und klicken Sie auf **OK**.

   Das Fenster **Liste der anstößigen Sprache** wird geöffnet.

8. Öffnen Sie mit dem Link **Hinzufügen** das Fenster **Verbotene Phrase**.

9. Geben Sie eine vollständige Phrase oder eine entsprechende Maske ein, legen Sie einen gewichteten Koeffizienten für die Phrase fest und klicken Sie auf **OK**.

Damit eine bestimmte Maske nicht mehr verwendet wird, muss sie nicht gelöscht werden. Es ist ausreichend, im Fenster **Liste der anstößigen Sprache** das entsprechende Kontrollkästchen zu deaktivieren.

VERBOTENE UND ERLAUBTE ABSENDER

Zur Liste der *verbotenen Absender* können Sie Absenderadressen hinzufügen, deren Nachrichten von Anti-Spam als Spam identifiziert wurden. Absenderadressen, von denen kein Spam erwartet wird, stehen auf der Liste der *erlaubten Absender*. Diese Liste wird beim Training der Komponente Anti-Spam (s. Abschnitt "Adressen zur Liste der erlaubten Absender hinzufügen" auf S. 124) automatisch angelegt. Außerdem können Sie der Liste Einträge hinzufügen.

In die Listen für erlaubte und verbotene Absender können vollständige Adressen und Adressmasken eingetragen werden (s. Abschnitt "Spam nach Phrasen und Adressen ermitteln. Listen erstellen" auf S. 125).

Gehen Sie folgendermaßen vor, um eine Liste mit erlaubten oder verbotenen Absendern zu erstellen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
5. Führen Sie im nächsten Fenster auf der Registerkarte **Allgemein** folgende Aktionen aus:
   - Wenn eine Liste für verbotene Absender erstellt werden soll, aktivieren Sie im Block **Folgende Nachrichten als Spam einstufen** das Kontrollkästchen **Von verbotenen Absendern** und klicken Sie rechts auf **Auswählen**.

     Das Fenster **Liste mit verbotenen Absendern** wird geöffnet.
   - Wenn eine Liste für erlaubte Absender erstellt werden soll, aktivieren Sie im Block **Folgende Nachrichten als erwünscht einstufen** das Kontrollkästchen **Von erlaubten Absendern** und klicken Sie rechts auf **Auswählen**.

     Das Fenster **Liste mit erlaubten Absendern** wird geöffnet.
6. Öffnen Sie mit dem Link **Hinzufügen** das Fenster **Adressmaske für E-Mails**.
7. Geben Sie eine Adressmaske ein und klicken Sie auf **OK**.

Damit eine bestimmte Maske nicht mehr verwendet wird, muss sie nicht gelöscht werden. Es ist ausreichend, im Fenster mit der Liste das entsprechende Kontrollkästchen zu deaktivieren.

IHRE ADRESSEN

Sie können eine Liste mit Ihren E-Mail-Adressen anlegen, damit nicht an Sie adressierte Mails als Spam markiert werden

Gehen Sie folgendermaßen vor, um eine Liste mit Ihren Adressen anzulegen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
5. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Allgemein** das Kontrollkästchen **Nicht an mich adressiert** und klicken Sie auf **Meine Adressen**.

   Das Fenster **Meine Adressen** wird geöffnet.

6. Öffnen Sie mit dem Link **Hinzufügen** das Fenster **Adressmaske für E-Mails**.

7. Geben Sie eine Adressmaske ein und klicken Sie auf **OK**.

Damit eine bestimmte Maske nicht mehr verwendet wird, muss sie nicht gelöscht werden. Es ist ausreichend, im Fenster **Meine Adressen** das entsprechende Kontrollkästchen zu deaktivieren.

PHRASEN UND ADRESSEN EXPORTIEREN UND IMPORTIEREN

Listen mit Phrasen und Adressen können flexibel eingesetzt werden. Zum Beispiel können Adressen in eine entsprechende Liste auf einem anderen Computer übertragen werden, auf dem Kaspersky PURE installiert ist.

Dabei gilt folgendes Vorgehen:

1. *Exportieren* Sie eine Liste, d.h. die Einträge werden aus einer Liste in eine Datei kopiert.

2. Übertragen Sie die gespeicherte Datei auf einen anderen Computer (z.B. per E-Mail oder mit einem Wechseldatenträger).

3. *Importieren* Sie eine Liste, d.h. die Einträge werden aus einer Datei in eine analoge Liste auf einem anderen Computer eingetragen.

Beim Export einer Liste können Sie auswählen, ob nur die gewählten Listenelemente oder die gesamte Liste kopiert werden soll. Beim Import können der Liste neue Elemente hinzugefügt oder die vorhandene Liste durch eine importierte ersetzt werden.

➧ *Gehen Sie folgendermaßen vor, um die Einträge aus einer Liste zu exportieren:*

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.

4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.

5. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Allgemein** das Kontrollkästchen in der Zeile mit dem Namen der Liste, aus der die Einträge exportiert werden sollen. Klicken Sie dann rechts auf die entsprechende Schaltfläche.

6. Aktivieren Sie im folgenden Fenster in der Liste die Kontrollkästchen für die Einträge, die in die Datei aufgenommen werden sollen.

7. Klicken Sie auf den Link **Export**.

   Im folgenden Fenster können Sie wählen, welche Elemente exportiert werden sollen. Führen Sie hier eine der folgenden Aktionen aus:

   - Klicken Sie auf **Ja**, wenn nur ausgewählte Einträge in die Datei aufgenommen werden sollen.

   - Klicken Sie auf **Nein**, wenn die gesamte Liste aufgenommen werden soll.

8. Geben Sie im folgenden Fenster einen Typ und einen Namen für die zu speichernde Datei an und bestätigen Sie das Speichern.

➧ *Gehen Sie folgendermaßen vor, um die Einträge aus einer Datei in eine Liste zu importieren:*

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.

4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.

5. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Allgemein** das Kontrollkästchen in der Zeile mit dem Namen der Liste, in die die Einträge importiert werden sollen. Klicken Sie dann rechts auf die entsprechende Schaltfläche.

6. Klicken Sie im Fenster auf den Link **Import**. Wenn Sie eine Liste mit erlaubten Absendern importieren, wählen Sie im folgenden Menü den Punkt **Aus Datei importieren**. Für die übrigen Listen muss kein Menüpunkt gewählt werden.

   Wenn die Liste nicht leer ist, wird Ihnen im folgenden Fenster vorgeschlagen, die zu importierenden Elemente hinzuzufügen. Führen Sie hier eine der folgenden Aktionen aus:

   - Klicken Sie auf **Ja**, wenn die Dateieinträge zur Liste hinzugefügt werden sollen.
   - Klicken Sie auf **Nein**, wenn die vorhandenen Einträge durch die Liste aus der Datei ersetzt werden sollen.

7. Wählen Sie im folgenden Fenster eine Datei mit den zu importierenden Einträgen.

Liste mit erlaubten Absendern aus einem Adressbuch importieren

Für Adressen aus der Liste erlaubter Absender ist der Import von Adressen oder eines Adressbuchs für Microsoft Office Outlook / Microsoft Outlook Express (Windows Mail) möglich.

Gehen Sie folgendermaßen vor, um eine Liste mit erlaubten Absendern aus einem Adressbuch zu importieren:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.

4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.

5. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Allgemein** im Block **Folgende Nachrichten als nützlich einstufen** das Kontrollkästchen **Von erlaubten Absendern** und klicken Sie auf **Auswählen**.

   Das Fenster **Liste mit erlaubten Absendern** wird geöffnet.

6. Klicken Sie auf den Link **Import**, öffnen Sie das Menü zur Auswahl einer Quelle und wählen Sie den Punkt **Aus Adressbuch importieren**.

7. Wählen Sie im folgenden Fenster das entsprechende Adressbuch.

GRENZWERTE FÜR DEN SPAM-FAKTOR REGULIEREN

Die Spam-Erkennung basiert auf der Verwendung moderner Filtertechnologien, die es erlauben, Anti-Spam so zu trainieren (s. Abschnitt "Anti-Spam-Training" auf S. 122), dass er relativ genau zwischen Spam, potentiellem Spam und erwünschten Mails unterscheiden kann. Dabei erhält jedes Element einer erwünschten oder einer Spam-Mail einen Koeffizienten.

Wenn eine E-Mail in Ihrer Mailbox eintrifft, untersucht Anti-Spam die Nachricht mit Hilfe der iBayes-Technologie auf das Vorhandensein von Elementen, die für Spam und erwünschte Post charakteristisch sind. Die Koeffizienten für jedes Element einer erwünschten oder einer Spam-Mail werden summiert, und ein *Spam-Faktor* wird errechnet. Je höher der Spam-Faktor, desto höher ist die Wahrscheinlichkeit, mit der es sich bei einer Nachricht um Spam handelt. In der Grundeinstellung gilt eine Nachricht mit einem Spam-Faktor bis 60 als erwünscht. Bei einem Spam-Faktor von über 60 gilt eine Nachricht als potentieller Spam. Wenn der Wert über 90 liegt, wird eine Nachricht als Spam betrachtet. Sie können die Grenzwerte für den Spam-Faktor ändern.

Gehen Sie folgendermaßen vor, um die Grenzwerte für den Spam-Faktor zu ändern:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.

4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.

5. Passen Sie im folgenden Fenster auf der Registerkarte **Algorithmus** im Block **Spam-Faktor** den Wert des Spam-Faktors an. Dazu dient der Schieberegler oder das Eingabefeld mit Pfeiltasten.

ZUSÄTZLICHE MERKMALE FÜR DIE SPAM-FILTERUNG VERWENDEN

Das Ergebnis für den Spam-Faktor kann durch zusätzliche Nachrichtenmerkmale beeinflusst werden: beispielsweise das Fehlen einer Empfängeradresse im Feld "An" oder eine zu lange Betreffzeile (über 250 Zeichen). Wenn eine Nachricht diese Merkmale aufweist, erhöht sich die Wahrscheinlichkeit, dass es sich um Spam handelt. Der Wert für den Spam-Faktor erhöht sich entsprechend. Sie können wählen, welche Zusatzmerkmale bei der Nachrichtenanalyse berücksichtigt werden sollen.

Gehen Sie folgendermaßen vor, um Zusatzmerkmale zu verwenden, die den Spam-Faktor erhöhen:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.

4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.

5. Klicken Sie im folgenden Fenster auf der Registerkarte **Algorithmus** auf **Erweitert**.

6. Aktivieren Sie im folgenden Fenster **Erweitert** das Kontrollkästchen für die Merkmale, die bei der Nachrichtenanalyse berücksichtigt werden sollen, um den Spam-Faktor zu erhöhen.

ALGORITHMUS ZUR SPAM-ERKENNUNG AUSWÄHLEN

Die Spam-Analyse von E-Mails erfolgt unter Verwendung von Algorithmen zum Erkennen.

- **Heuristische Analyse**. Anti-Spam analysiert die Nachrichten mit Hilfe heuristischer Regeln. Die heuristische Analyse wird immer verwendet.

- **Grafikanalyse (GSG)**. Die GSG-Technologie wird von Anti-Spam verwendet, um Spam in Form von Bildern zu identifizieren.

- **Analyse von angehängten Dokumenten im Format .rtf**. Anti-Spam analysiert die an Nachrichten angehängten Dokumente auf das Vorhandensein von Spam-Merkmalen.

- **Lernfähiger Algorithmus zur Textanalyse (iBayes)**. Mit dem iBayes-Algorithmus wird analysiert, wie häufig im Text einer Nachricht Wörter verwendet werden, die für Spam typisch sind. Aufgrund der Analyse wird eine Nachricht als erwünscht oder als Spam eingestuft. Vor der Verwendung des iBayes-Algorithmus ist ein Anti-Spam-Training erforderlich (s. Abschnitt "Anti-Spam-Training" auf S. 122).

Gehen Sie folgendermaßen vor, um bei der E-Mail-Analyse einen Spam-Erkennungsalgorithmus zu verwenden / nicht zu verwenden:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.

4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.

5. Aktivieren / deaktivieren Sie im folgenden Fenster auf der Registerkarte **Algorithmus** im Block **Erkennungsalgorithmen** die entsprechenden Kontrollkästchen.

MARKIERUNG ZUM BETREFF EINER NACHRICHT HINZUFÜGEN

Anti-Spam kann Nachrichten, die sich bei der Untersuchung als Spam oder potentieller Spam erweisen, im Feld **Betreff** spezielle Markierungen hinzufügen:

- **[!! SPAM]** – für Nachrichten, die als Spam identifiziert wurden.
- **[?? Probable Spam]** – für Nachrichten, die als potentieller Spam identifiziert wurden.

Solche Markierungen in der Betreffzeile können Ihnen bei der Durchsicht von Nachrichtenlisten behilflich sein, Spam und potentiellen Spam aufzufinden.

Gehen Sie folgendermaßen vor, damit Anti-Spam der Betreffzeile Markierungen hinzufügt / nicht hinzufügt:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
5. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Aktionen** die Kontrollkästchen für jener Markierungen, die dem Betreff hinzugefügt werden sollen. Wenn ein Kontrollkästchen angekreuzt wurde, kann der Markierungstext geändert werden. Deaktivieren Sie das entsprechende Kontrollkästchen, wenn keine Markierung erforderlich ist.

FILTERUNG VON E-MAILS AUF DEM SERVER. MAIL-MANAGER

Sie können eine Liste der E-Mails auf dem Server anzeigen, ohne die Nachrichten auf Ihren Computer herunterzuladen. Dadurch wird Ihnen erlaubt, den Empfang bestimmter Nachrichten abzulehnen, wodurch Sie nicht nur Zeit und Geld bei der Arbeit mit elektronischer Post sparen, sondern auch die Wahrscheinlichkeit des Downloads von Spam und Viren auf Ihren Computer reduzieren können.

Für die Arbeit mit E-Mails auf dem Server dient der *Mail-Manager*.

Das Fenster des Mail-Managers wird jedes Mal geöffnet, bevor E-Mails heruntergeladen werden (unter der Bedingung, dass er aktiviert ist).

Beachten Sie, dass das Fenster des Mail-Managers nur geöffnet wird, wenn E-Mails mit dem Protokoll POP3 empfangen werden. Der Mail-Manager wird nicht geöffnet, wenn der POP3-Server die Ansicht von E-Mail-Kopfzeilen nicht unterstützt oder alle auf dem Server vorhandenen E-Mails von Benutzern aus der Liste mit erlaubten Absendern stammen (s. S. 128).

Der mittlere Bereich des Manager-Fensters enthält eine Liste der E-Mails auf dem Server. Wählen Sie eine Nachricht aus der Liste, um Details aus ihrer Kopfzeile zu lesen.

Die Voransicht von Kopfzeilen kann beispielsweise in folgender Situation von Nutzen sein: Ein Spammer hat auf dem Computer Ihres Kollegen ein Schadprogramm installiert, das unter seinem Namen Spam verschickt und dabei das Adressbuch des Mailprogramms verwendet. Die Wahrscheinlichkeit, dass sich Ihre Adresse im Adressbuch eines Kollegen befindet, ist relativ hoch, was dazu führt, dass ein Schadprogramm Ihre Adresse mit Spam überhäuft.

In dieser Situation ist es unmöglich, aufgrund der Absenderadresse zu ermitteln, ob eine Nachricht wirklich von Ihrem Kollegen oder mit Hilfe eines Schadprogramms von einem Spammer geschickt wurde. Mit Hilfe des Nachrichtenheaders lässt sich feststellen, wann und von wem eine Nachricht gesendet wurde, wie groß sie ist und welche Route sie vom Absender bis in Ihren Briefkasten zurückgelegt hat. Die genannten Daten helfen Ihnen bei der Entscheidung, ob eine E-Mail wirklich vom Server heruntergeladen oder besser gelöscht werden sollte.

Gehen Sie folgendermaßen vor, um den Mail-Manager zu verwenden:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
5. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Eingehende Mails** das Kontrollkästchen **Mail-Manager bei Mailempfang mit POP3-Protokoll öffnen**.

Gehen Sie folgendermaßen vor, um E-Mails mit Hilfe des Mail-Managers vom Server zu löschen:

1. Vor dem Nachrichtenempfang öffnet sich das Fenster des Mail-Managers. Aktivieren Sie dort in der Spalte **Löschen** das Kontrollkästchen, das der Nachricht entspricht.
2. Klicken Sie im oberen Bereich des Fensters auf **Die markierten löschen**.

Die Nachrichten werden vom Server gelöscht. Dabei erhalten Sie eine Benachrichtigung, die als **[!! SPAM]** markiert und nach den Regeln Ihres Mailprogramms (s. Abschnitt "Spam-Verarbeitung in Mailprogrammen anpassen" auf S. 133) verarbeitet wird.

NACHRICHTEN FÜR MICROSOFT EXCHANGE SERVER VON DER UNTERSUCHUNG AUSSCHLIEßEN

Sie können E-Mails, die im Rahmen eines internen Netzwerks (z.B. Firmenpost) verschickt werden, von der Spam-Untersuchung ausschließen. Beachten Sie, dass dann E-Mails als interne Mail betrachtet werden, wenn als Mail-Client auf allen Netzwerkcomputern das Programm Microsoft Office Outlook benutzt wird und die Mailboxen der Benutzer sich auf einem Exchange-Server oder auf den Servern, die mit X400-Konnektoren verbunden sind, befinden.

In der Grundeinstellung werden Nachrichten für Microsoft Exchange Server nicht von Anti-Spam untersucht.

Gehen Sie folgendermaßen vor, damit Anti-Spam die Nachrichten für Microsoft Exchange Server analysiert:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
4. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
5. Deaktivieren Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Ausnahmen** das Kontrollkästchen **E-Mails für Microsoft Exchange Server nicht untersuchen**.

SPAM-VERARBEITUNG IN MAILPROGRAMMEN ANPASSEN

Wenn sich aufgrund einer Untersuchung ergibt, dass eine Nachricht als Spam oder potentieller Spam gilt, sind die weiteren Aktionen von Anti-Spam vom Status der Nachricht und von der gewählten Aktion abhängig. Standardmäßig werden E-Mails, die als Spam oder potentieller Spam gelten, modifiziert: Einer Nachricht wird im Feld **Betreff** die Markierung **[!! SPAM]** oder **[?? Probable Spam]** hinzugefügt (s. Abschnitt "Markierung zum Betreff einer Nachricht hinzufügen" auf S. 132).

Sie können Zusatzaktionen für Spam und potentiellen Spam festlegen. In den Mailprogrammen Microsoft Office Outlook und Microsoft Outlook Express (Windows Mail) sind dafür spezielle Erweiterungsmodule vorgesehen. Für die Mailprogramme The Bat! und Thunderbird können Sie Filterregeln erstellen.

IN DIESEM ABSCHNITT

Microsoft Office Outlook 134

Microsoft Outlook Express (Windows Mail) 134

Regel für die Spam-Untersuchung von Nachrichten erstellen 134

The Bat! 135

Thunderbird 135

MICROSOFT OFFICE OUTLOOK

E-Mails, die Anti-Spam als Spam oder potentieller Spam klassifiziert, werden im Feld **Betreff** standardmäßig durch die Markierungen **[!! SPAM]** oder **[?? Probable Spam]** gekennzeichnet. Wenn es erforderlich ist, Nachrichten nach der Untersuchung durch Anti-Spam zusätzlich zu verarbeiten, können Sie Microsoft Office Outlook entsprechend anpassen. Das Einstellungsfenster für die Spam-Bearbeitung erscheint automatisch, wenn das Mailprogramm nach der Installation von Kaspersky PURE zum ersten Mal gestartet wird. Die Einstellungen für die Verarbeitung von Spam und potentiellen Spam stehen außerdem in Microsoft Office Outlook auf der speziellen Registerkarte **Anti-Spam** im Menü **Extras** → **Optionen** zur Verfügung.

MICROSOFT OUTLOOK EXPRESS (WINDOWS MAIL)

E-Mails, die Anti-Spam als Spam oder potentieller Spam klassifiziert, werden im Feld **Betreff** standardmäßig durch die Markierungen **[!! SPAM]** oder **[?? Probable Spam]** gekennzeichnet. Wenn es erforderlich ist, Nachrichten nach der Untersuchung durch Anti-Spam zusätzlich zu verarbeiten, können Sie Microsoft Office Outlook (Windows Mail) entsprechend anpassen.

Das Einstellungsfenster für die Spam-Verarbeitung erscheint, wenn das Mailprogramm nach der Installation der Anwendung zum ersten Mal gestartet wird. Es kann auch mit der Schaltfläche **Einstellungen** geöffnet werden, die sich neben den Schaltflächen **Spam** und **Kein Spam** auf der Symbolleiste befindet.

REGEL FÜR DIE SPAM-UNTERSUCHUNG VON NACHRICHTEN ERSTELLEN

Im Folgenden wird erklärt, wie Spam-Regeln für die Nachrichtenverarbeitung mit Anti-Spam im Mailprogramm Microsoft Office Outlook erstellt werden. Auf Basis dieser Anleitung können Sie eine eigene Regel erstellen.

Gehen Sie folgendermaßen vor, um eine Regel zur Spam-Verarbeitung von Nachrichten zu erstellen:

1. Starten Sie das Programm Microsoft Office Outlook und verwenden Sie den Befehl **Extras** → **Regeln und Benachrichtigungen** im Programmhauptfenster. Die Methode für den Start des Assistenten ist von der Microsoft Office Outlook-Version abhängig, die Sie verwenden. In dieser Hilfe wird das Erstellen einer Regel mit Hilfe von Microsoft Office Outlook 2003 beschrieben.

2. Gehen Sie im Fenster **Regeln und Benachrichtigungen** auf die Registerkarte **Regeln für E-Mails** und klicken Sie auf **Neu**. Dadurch wird der Assistent zum Erstellen einer neuen Regel gestartet. Er besteht aus einer Folge von Fenstern / Schritten:

   a. Sie können auswählen, ob zum Erstellen der Regel eine Vorlage benutzt werden soll oder nicht. Wählen Sie die Variante **Regel ohne Vorlage erstellen** und wählen Sie als Prüfungsbedingung **Nachrichten bei Ankunft prüfen**. Klicken Sie auf **Weiter**.

   b. Klicken Sie im Fenster zur Auswahl der Bedingungen für die Nachrichtenprüfung auf **Weiter**, ohne ein Kontrollkästchen zu aktivieren. Bestätigen Sie in der Bestätigungsanfrage die Anwendung dieser Regel auf alle Nachrichten, die Sie erhalten.

   c. Aktivieren Sie im Fenster zur Auswahl der Aktionen für die Nachrichten in der Aktionsliste das Kontrollkästchen **diese mit einer vordefinierten Aktion bearbeiten**. Klicken Sie im unteren Bereich des Fensters auf den Link **einer vordefinierten Aktion**. Wählen Sie aus der Dropdown-Liste den Wert **Kaspersky Anti-Spam** und klicken Sie auf **OK**.

d. Klicken Sie im Fenster zur Auswahl von Ausnahmen auf **Weiter**, ohne ein Kontrollkästchen zu aktivieren.

e. Im Fenster zum Abschluss der Regelerstellung können Sie den Namen der Regel ändern (standardmäßig lautet er Kaspersky Anti-Spam). Überprüfen Sie, ob das Kontrollkästchen **Diese Regel aktivieren** aktiviert ist und klicken Sie auf **Fertig**.

3. Die neue Regel wird standardmäßig an erste Stelle zur Regelliste im Fenster **Regeln und Benachrichtigungen** hinzugefügt. Wenn Sie möchten, dass die Regel zuletzt auf eine Nachricht angewandt wird, verschieben Sie sie an das Ende der Liste.

Alle Nachrichten, die in der Mailbox ankommen, werden auf der Grundlage von Regeln bearbeitet. Die Verwendungsreihenfolge der Regeln hängt von der Priorität ab, die den einzelnen Regeln zugewiesen wurde. Die Regeln werden nacheinander verwendet, wobei mit der obersten Regel begonnen wird und die Priorität der Regeln nach unten sinkt. Sie können die Anwendungspriorität der Regeln für Nachrichten erhöhen oder senken. Dazu wird eine Regel in der Liste nach oben oder unten verschoben. Wenn Sie nicht möchten, dass eine Nachricht zusätzlich nach einer Anti-Spam-Regel bearbeitet wird, nachdem bereits eine Regel angewandt wurde, muss in den Parametern dieser Regel das Kontrollkästchen **keine weiteren Regeln anwenden** aktiviert werden (s. Schritt 3. zum Erstellen der Regel).

THE BAT!

Die Aktionen für Spam und potentiellen Spam werden im Mailprogramm The Bat! mit den Mitteln des Mailprogramms festgelegt.

➧ *Gehen Sie folgendermaßen vor, um in The Bat! die Spam-Verarbeitungsregeln anzupassen:*

1. Wählen Sie im Menü **Optionen** des Mailprogramms den Punkt **Benutzereinstellungen**.

2. Wählen Sie in der Konfigurationsstruktur das Objekt **Spam-Schutz**.

Die angezeigten Parameter für den Spam-Schutz gelten für alle auf dem Computer installierten Anti-Spam-Module, die die Arbeit mit The Bat! unterstützen.

Sie müssen eine Score-Stufe festlegen und die Aktion angeben, die auf Nachrichten angewandt werden soll, denen ein bestimmter Score zugewiesen wurde (im Fall von Anti-Spam ist das die Wahrscheinlichkeit, dass eine E-Mail als Spam gilt):

- Nachricht mit einem Score, der den Grenzwert überschreitet, löschen.
- Nachricht mit einem bestimmten Score in einen speziellen Ordner für Spam-Nachrichten verschieben.
- Spam-Nachrichten, die mit einer speziellen Kopfzeile markiert sind, in den Spam-Ordner verschieben.
- Spam-Nachrichten im Ordner **Eingang** belassen.

Aufgrund der Bearbeitung von E-Mail-Nachrichten durch Kaspersky PURE wird der Nachricht auf der Basis eines Faktors, den Sie festlegen können, der Status Spam oder potentieller Spam zugewiesen. Im Mailprogramm The Bat! ist ein entsprechender Score-Algorithmus für Nachrichten realisiert, der den Gegenstand Spam betrifft, und ebenfalls auf dem Spam-Faktor basiert. Um Differenzen zwischen den Spam-Faktoren in Kaspersky PURE und in The Bat! zu vermeiden, werden alle von Anti-Spam geprüften Nachrichten dem Rating angepasst, das dem Status der Nachricht entspricht: erwünschte E-Mails – 0%, potentieller Spam – 50%, Spam – 100%. Dadurch stimmt der Score der Nachricht im Mailprogramm The Bat! nicht mit dem in Anti-Spam festgelegten Spam-Faktor überein, sondern mit dem Faktor des entsprechenden Status.

Einzelheiten über den Spam-Score und die Verarbeitungsregeln s. Dokumentation zum Mailprogramm The Bat!.

THUNDERBIRD.

E-Mails, die Anti-Spam als Spam oder potentieller Spam klassifiziert, werden im Feld **Betreff** standardmäßig durch die Markierungen **[!! SPAM]** oder **[?? Probable Spam]** gekennzeichnet. Wenn nach der Untersuchung durch Anti-Spam eine zusätzliche Nachrichtenverarbeitung erforderlich ist, können Sie Thunderbird entsprechend anpassen. Öffnen Sie dazu mit dem Menübefehl **Extras** → **Filter** das Konfigurationsfenster (für Details über die Arbeit mit dem Mail-Client schlagen Sie in der Hilfe zu Mozilla Thunderbird nach).

Das Anti-Spam-Erweiterungsmodul für Thunderbird erlaubt es, ein Training mit E-Mails vorzunehmen, die mit diesem Mail-Client empfangen und gesendet wurden. Außerdem kann die E-Mail-Korrespondenz auf Spam untersucht werden. Das Modul wird in Thunderbird integriert und leitet E-Mails zur Untersuchung an die Komponente Anti-Spam um. Dazu dient der Menübefehl **Extras** → **Junk-Filter auf Ordner anwenden**. Die Nachrichtenuntersuchung wird also nicht von Thunderbird, sondern von Kaspersky PURE ausgeführt. Dabei bleibt die Funktionalität von Thunderbird unverändert.

Der Status des Anti-Spam-Erweiterungsmoduls wird in Form eines Symbols in der Statuszeile von Thunderbird angezeigt. Das graue Symbol bedeutet, dass bei der Arbeit des Plug-ins ein Problem vorliegt oder dass die Komponente Anti-Spam deaktiviert wurde. Das Konfigurationsfenster von Kaspersky PURE kann durch Doppelklick auf das Symbol geöffnet werden. Um zu den Einstellungen für Anti-Spam zu gelangen, klicken Sie im Block **Anti-Spam** auf **Einstellungen.**

ANTI-BANNER

Anti-Banner dient dazu, die Anzeige von Bannern auf den von Ihnen besuchten Webseiten und im Interface bestimmter Computerprogramme zu blockieren. Bannerwerbung kann Sie von der Arbeit ablenken und verursacht erhöhten Datenverkehr.

Bevor ein Banner auf einer Webseite oder im Fenster eines Computerprogramms angezeigt wird, muss es aus dem Internet geladen werden. Anti-Banner prüft die Adresse, von der ein Banner geladen wird. Stimmt die Adresse mit einer Maske aus der im Lieferumfang von Kaspersky PURE enthaltenen Liste oder der von Ihnen angelegten Schwarzen Bannerliste überein, dann wird das Banner blockiert. Zum Sperren von Bannern, deren Adressmasken nicht in den genannten Listen enthalten sind, wird eine heuristische Analyse verwendet.

Zusätzlich kann eine Weiße Adressenliste angelegt werden, auf deren Basis die Banneranzeige erlaubt wird.

IN DIESEM ABSCHNITT

Anti-Banner aktivieren und deaktivieren 136

Untersuchungsmethoden wählen 137

Listen für verbotene und erlaubte Banneradressen erstellen 137

Adressenlisten exportieren / importieren 137

ANTI-BANNER AKTIVIEREN UND DEAKTIVIEREN

Anti-Banner ist standardmäßig aktiviert und arbeitet im optimalen Modus. Bei Bedarf kann Anti-Banner deaktiviert werden.

Gehen Sie folgendermaßen vor, um Anti-Banner zu aktivieren oder zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Banner**.
4. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Anti-Banner aktivieren**, um die Komponente auszuschalten. Aktivieren Sie dieses Kontrollkästchen, um die Komponente einzuschalten.

UNTERSUCHUNGSMETHODEN WÄHLEN

Sie können die Methoden festlegen, mit denen Anti-Banner Adressen untersuchen soll, von denen Banner geladen werden können: Zusätzlich zu diesen Methoden untersucht Anti-Banner die Banneradressen auf Übereinstimmung mit Masken aus den Listen für erlaubte und verbotene Adressen, falls diese Listen verwendet werden.

Gehen Sie folgendermaßen vor, um festzulegen, mit welchen Methoden Anti-Banner Adressen untersuchen soll:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Banner**.
4. Aktivieren Sie auf der rechten Fensterseite in der Gruppe **Untersuchungsmethoden** die Kontrollkästchen der zu verwendenden Methoden.

LISTEN FÜR VERBOTENE UND ERLAUBTE BANNERADRESSEN ERSTELLEN

Mit Hilfe von Listen für verbotene und erlaubte Banneradressen können Sie festlegen, von welchen Adressen das Laden und die Anzeige von Bannern verboten bzw. erlaubt werden soll. Anti-Banner blockiert den Download und die Anzeige der Banner von Adressen, die den Masken entsprechen, die auf der von Ihnen angelegten Schwarzen Liste stehen. Anti-Banner erlaubt den Download und die Anzeige der Banner von Adressen, die den Masken entsprechen, die auf der von Ihnen angelegten Weißen Liste stehen.

Gehen Sie folgendermaßen vor, um eine Maske zur Liste der verbotenen oder erlaubten Adressen hinzuzufügen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Banner**.
4. Aktivieren Sie im rechten Fensterbereich im Block **Erweitert** das Kontrollkästchen **Schwarze Adressenliste verwenden** (oder **Weiße Adressenliste verwenden**) und klicken Sie rechts von diesem Kontrollkästchen auf **Einstellungen**.

   Das Fenster **Schwarze Liste** (oder **Weiße Liste**) wird geöffnet.
5. Verwenden Sie den Link **Hinzufügen**, um das Fenster **Adressmaske (URL)** zu öffnen.
6. Geben Sie die Maske einer verbotenen (oder erlaubten) Banneradresse ein und klicken Sie auf **OK**.

Damit eine bestimmte Maske nicht mehr verwendet wird, muss sie nicht gelöscht werden. Es ist ausreichend, im Fenster mit der Liste das entsprechende Kontrollkästchen zu deaktivieren.

ADRESSENLISTEN EXPORTIEREN / IMPORTIEREN

Listen für verbotene und erlaubte Banneradressen können mehrfach eingesetzt werden. Banneradressen können beispielsweise in eine entsprechende Liste auf einem anderen Computer übertragen werden, auf dem Kaspersky PURE installiert ist.

Dabei gilt folgendes Vorgehen:

1. *Exportieren* Sie eine Liste, d.h. die Einträge werden aus einer Liste in eine Datei kopiert.
2. Übertragen Sie die gespeicherte Datei auf einen anderen Computer (z.B. per E-Mail oder mit einem Wechseldatenträger).

3. *Importieren* Sie eine Liste, d.h. die Einträge werden aus einer Datei in eine analoge Liste auf einem anderen Computer eingetragen.

Beim Export einer Liste können Sie auswählen, ob nur die gewählten Listenelemente oder die gesamte Liste kopiert werden soll. Beim Import können der Liste neue Elemente hinzugefügt oder die vorhandene Liste durch eine importierte ersetzt werden.

Gehen Sie folgendermaßen vor, um Banneradressen aus der Liste für erlaubte oder verbotene Banneradressen zu exportieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Banner**.
4. Klicken Sie auf der rechten Fensterseite im Block **Erweitert** in der Zeile mit dem Namen der Liste, aus der Adressen in eine Datei kopiert werden sollen, auf **Einstellungen**.
5. Aktivieren Sie im folgenden Fenster **Weiße Liste** (oder **Schwarze Liste**) die Kontrollkästchen der Adressen, die in die Datei aufgenommen werden sollen.
6. Klicken Sie auf **Export**.

   Im folgenden Fenster können Sie wählen, welche Elemente exportiert werden sollen. Führen Sie hier eine der folgenden Aktionen aus:

   - Klicken Sie auf **Ja**, wenn nur ausgewählte Adressen in die Datei aufgenommen werden sollen.
   - Klicken Sie auf **Nein**, wenn die gesamte Liste in die Datei aufgenommen werden soll.
7. Geben Sie im folgenden Fenster einen Namen für die zu speichernde Datei ein und bestätigen Sie das Speichern.

Gehen Sie folgendermaßen vor, um Banneradressen aus einer Datei in eine Liste für erlaubte oder verbotene Adressen zu importieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Banner**.
4. Klicken Sie auf der rechten Fensterseite im Block **Erweitert** in der Zeile mit dem Namen der Liste, zu der Adressen aus einer Datei hinzugefügt werden sollen, auf **Einstellungen**.
5. Klicken Sie im folgenden Fenster **Schwarze Liste** (oder **Weiße Liste**) auf **Import**.

   Wenn die Liste nicht leer ist, wird Ihnen im folgenden Fenster vorgeschlagen, die zu importierenden Elemente hinzuzufügen. Führen Sie hier eine der folgenden Aktionen aus:

   - Klicken Sie auf **Ja**, wenn die Dateieinträge zur Liste hinzugefügt werden sollen.
   - Klicken Sie auf **Nein**, wenn die vorhandenen Einträge durch die Liste aus der Datei ersetzt werden sollen.
6. Wählen Sie im folgenden Fenster eine Datei mit den zu importierenden Einträgen.

PROGRAMMKONTROLLE

Die Programmkontrolle hindert Programme daran, systemgefährliche Aktionen auszuführen, und kontrolliert den Zugriff auf Betriebssystemressourcen und auf Ihre persönlichen Daten.

Die Komponente verfolgt die Aktionen, die von auf dem Computer installierten Programmen im System ausgeführt werden, und reguliert ihre Aktivität entsprechend den Regeln der Programmkontrolle. Diese Regeln regulieren eine potentiell gefährliche Aktivität. Dazu zählt der Zugriff der Programme auf geschützte Ressourcen (Dateien und Ordner, Registrierungsschlüssel, Netzwerkadressen usw.).

Die Netzwerkaktivität von Programmen wird von der Komponente Firewall kontrolliert.

Wenn ein Programm zum ersten Mal auf dem Computer gestartet wird, untersucht die Komponente Programmkontrolle seine Sicherheit und verschiebt das Programm in eine der Sicherheitsgruppen. Die Sicherheitsgruppe bestimmt die Regeln, die Kaspersky PURE zur Aktivitätskontrolle dieses Programms verwenden wird. Die Regeln der Programmkontrolle bestehen aus einer Auswahl von Rechten für den Zugriff auf Computerressourcen und von Beschränkungen für unterschiedliche Programmaktionen auf dem Computer.

Sie können die Bedingungen für die Zuordnung von Programmen zu den einzelnen Gruppen anpassen (s. S. 140), ein Programm in eine andere Gruppe verschieben (s. S. 141), und die Regeln für Kaspersky PURE ändern (s. S. 142).

Es wird empfohlen, am Kaspersky Security Network teilzunehmen (s. Abschnitt "Teilnahme an Kaspersky Security Network" auf S. 245), um die Optimierung der Programmkontrolle zu unterstützen. Die Daten, die mit Hilfe des Kaspersky Security Network ermittelt werden, erlauben es, Programme genauer zu einer bestimmten Sicherheitsgruppe zuzuordnen und optimale Regeln zur Programmkontrolle zu verwenden .

Beim wiederholten Start eines Programms kontrolliert die Programmkontrolle seine Integrität. Wenn ein Programm nicht verändert wurde, wendet die Komponente die aktuellen Regeln darauf an. Wenn ein Programm verändert wurde, überprüft die Programmkontrolle es erneut wie beim ersten Start.

Um den Zugriff von Programmen auf unterschiedliche Ressourcen des Computers zu kontrollieren, können Sie die vorgegebene Liste für geschützte Ressourcen verwenden oder die Liste durch benutzerdefinierte Ressourcen erweitern (s. S. 146).

IN DIESEM ABSCHNITT

Programmkontrolle aktivieren und deaktivieren 139

Programme zu Gruppen zuordnen 140

Aktivität von Programmen anzeigen 141

Sicherheitsgruppe ändern 141

Regeln für die Programmkontrolle 142

Schutz für Betriebssystemressourcen und persönliche Daten 146

PROGRAMMKONTROLLE AKTIVIEREN UND DEAKTIVIEREN

Standardmäßig ist die Programmkontrolle aktiviert und arbeitet in einem von Kaspersky Lab entwickelten Modus, Sie können sie jedoch bei Bedarf deaktivieren.

Gehen Sie folgendermaßen vor, um die Programmkontrolle zu aktivieren oder zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.
4. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Programmkontrolle aktivieren**, um die Komponente auszuschalten. Aktivieren Sie dieses Kontrollkästchen, um die Komponente einzuschalten.

PROGRAMME ZU GRUPPEN ZUORDNEN

Wenn ein Programm zum ersten Mal auf dem Computer gestartet wird, untersucht die Komponente Programmkontrolle seine Sicherheit und verschiebt das Programm in eine der Sicherheitsgruppen.

Auf der ersten Etappe zur Überprüfung eines Programms durchsucht Kaspersky PURE eine interne Datenbank für bekannte Programme nach einem Eintrag über das Programm und schickt anschließend eine Anfrage an die Datenbank des Kaspersky Security Network (sofern eine Internetverbindung besteht). Wenn in der Datenbank ein Eintrag zum Programm gefunden wird, wird das Programm in die Gruppe verschoben, die in der Datenbank angegeben ist.

Programme, die keine Gefahr für das System darstellen, werden in die Gruppe **Vertrauenswürdig** verschoben. In diese Gruppe werden standardmäßig solche Programme verschoben, die eine digitale Signatur besitzen oder deren übergeordnetes Objekt eine digitale Signatur besitzt.

Für Programme, die in der Datenbank von Kaspersky Security Network enthalten sind oder eine digitale Signatur besitzen, können Sie das automatische Verschieben in die Gruppe **Vertrauenswürdig** deaktivieren.

Das Verhalten von Programmen, die von der Programmkontrolle in die Gruppe **Vertrauenswürdig** verschoben werden, wird trotzdem von der Komponente Proaktiver Schutz kontrolliert.

Um die entsprechenden Gruppen für unbekannte Programme zu ermitteln (Programme, die nicht in der Datenbank von Kaspersky Security Network enthalten sind und keine digitale Signatur besitzen), verwendet Kaspersky PURE standardmäßig eine heuristische Analyse. Bei dieser Analyse erfolgt eine Risikobewertung des Programms, auf deren Basis das Programm in eine bestimmte Gruppe verschoben wird. Anstelle einer heuristischen Analyse können Sie eine Gruppe festlegen, in die Kaspersky PURE alle unbekannten Programme automatisch verschieben soll.

Die Programmkontrolle untersucht ein Programm standardmäßig im Verlauf von 30 Sekunden. Wenn die Risikobewertung innerhalb dieses Zeitraums nicht abgeschlossen wurde, wird das Programm in die Gruppe **Schwach beschränkt** verschoben und die Risikobewertung wird im Hintergrundmodus fortgesetzt. Anschließend wird das Programm endgültig in eine Gruppe verschoben. Sie können die Dauer ändern, für die gestartete Programme untersucht werden sollen. Wenn Sie sicher sind, dass alle Programme, die auf Ihrem Computer gestartet werden, sicher sind, können Sie die für die Untersuchung vorgesehene Dauer verringern. Sollten Sie riskante Software auf dem Computer installieren, so wird empfohlen, die Untersuchungsdauer zu erhöhen.

Wenn sich ein hoher Risikowert ergibt, werden Sie von Kaspersky PURE darüber informiert und Sie können eine Gruppe wählen, der das Programm zugeordnet werden soll. Die Meldung enthält eine Statistik über die Verwendung dieses Programms durch die Teilnehmer von Kaspersky Security Network. Diese Statistik und ein Verlauf über die Aktivitäten des Programms auf Ihrem Computer unterstützen Sie bei einer möglichst objektiven Entscheidung darüber, in welche Gruppe das Programm verschoben werden soll.

- *Gehen Sie folgendermaßen vor, um für Programme, die in der Datenbank von Kaspersky Security Network enthalten sind oder eine digitale Signatur besitzen, das automatische Verschieben in die Gruppe **Vertrauenswürdig** zu deaktivieren:*

  1. Öffnen Sie das Programmhauptfenster.
  2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
  3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.
  4. Deaktivieren Sie im rechten Fensterbereich im Block **Vertrauenswürdige Programme** die Kontrollkästchen **Mit digitaler Signatur** und **Die in der Datenbank von Kaspersky Security Network enthalten sind**.

- *Gehen Sie folgendermaßen vor, um die heuristische Analyse zur Ermittlung der Gruppen für unbekannte Programme zu verwenden:*

  1. Öffnen Sie das Programmhauptfenster.
  2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
  3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.

4. Wählen Sie im rechten Fensterbereich im Block **Vertrauenswürdige Programme** die Variante **Zur Ermittlung einer Gruppe die heuristische Analyse verwenden**.

Gehen Sie folgendermaßen vor, um die Dauer zu ändern, die zur Ermittlung einer Gruppe für ein Programm vorgesehen ist:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.
4. Ändern Sie im rechten Fensterbereich im Block **Erweitert** den Parameterwert **Maximale Dauer für die Ermittlung einer Programmgruppe**.

Gehen Sie folgendermaßen vor, damit alle unbekannten Programme in eine festgelegte Gruppe verschoben werden:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.
4. Wählen Sie im rechten Fensterbereich im Block **Vertrauenswürdige Programme** die Variante **Automatisch verschieben in die Gruppe** und wählen Sie die entsprechende Gruppe aus der Dropdown-Liste.

AKTIVITÄT VON PROGRAMMEN ANZEIGEN

Angezeigt werden können Informationen über alle Programme, die auf Ihrem Computer verwendet werden, und über alle Prozesse, die momentan ausgeführt werden.

Gehen Sie folgendermaßen vor, um eine Übersicht über die Programmaktivität anzuzeigen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.

   Das Fenster **Computersicherheit** wird geöffnet.
2. Wählen Sie auf der linken Seite des Fensters den Abschnitt **Programmkontrolle**.
3. Klicken Sie im rechten Fensterbereich auf den Link **Programmaktivität**.
4. Wählen Sie im folgenden Fenster **Programmaktivität** in der Liste **Kategorie** die entsprechende Programmkategorie aus.

SICHERHEITSGRUPPE ÄNDERN

Wenn ein Programm zum ersten Mal gestartet wird, verschiebt Kaspersky PURE das Programm automatisch in die entsprechende Gruppe (s. Abschnitt "Programme zu Sicherheitsgruppen zuordnen" auf S. 140). Falls erforderlich, können Sie ein Programm manuell in eine andere Gruppe verschieben.

Die Kaspersky-Lab-Experten warnen davor, Programme aus den Gruppen, denen sie automatisch zugewiesen wurden, in andere Gruppen zu verschieben. Ändern Sie stattdessen bei Bedarf die Regeln für ein bestimmtes Programm (s. Abschnitt "Programmregeln ändern" auf S. 143).

Gehen Sie folgendermaßen vor, um ein Programm in eine andere Gruppe zu verschieben:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.

Das Fenster **Computersicherheit** wird geöffnet.

2. Wählen Sie auf der linken Seite des Fensters den Abschnitt **Programmkontrolle**.
3. Klicken Sie im rechten Fensterbereich auf den Link **Programmaktivität**.
4. Wählen Sie im folgenden Fenster **Programmaktivität** in der Liste **Kategorie** die entsprechende Programmkategorie aus.
5. Öffnen Sie durch Rechtsklick das Kontextmenü des betreffenden Programms und wählen Sie dort den Punkt **Verschieben in Gruppe → <Name der Gruppe>**.

Gehen Sie folgendermaßen vor, um ein Programm wieder in die Standardgruppe zu verschieben:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.

   Das Fenster **Computersicherheit** wird geöffnet.
2. Wählen Sie auf der linken Seite des Fensters den Abschnitt **Programmkontrolle**.
3. Klicken Sie im rechten Fensterbereich auf den Link **Programmaktivität**.
4. Wählen Sie im folgenden Fenster **Programmaktivität** in der Liste **Kategorie** die entsprechende Programmkategorie aus.
5. Öffnen Sie durch Rechtsklick das Kontextmenü für das betreffende Programm und wählen Sie den Punkt **Standardgruppe wiederherstellen → <Name der Gruppe>**.

REGELN FÜR DIE PROGRAMMKONTROLLE

Die Regeln der Programmkontrolle bestehen aus einer Auswahl von Rechten für den Zugriff auf Computerressourcen und von Beschränkungen für unterschiedliche Programmaktionen auf dem Computer.

In der Grundeinstellung werden für die Programmkontrolle die Regeln jener Sicherheitsgruppe verwendet, in die ein Programm bei seinem ersten Start von Kaspersky PURE verschoben wurde. Die Gruppenregeln wurden von Kaspersky-Lab-Experten erarbeitet, um eine optimale Kontrolle der Programmaktivität zu gewährleisten. Bei Bedarf können Sie diese Regeln ändern oder sie für ein bestimmtes Programm anpassen. Regeln für ein Programm besitzen eine höhere Priorität als Regeln für eine Gruppe.

IN DIESEM ABSCHNITT

Gruppenregeln ändern 142

Programmregeln ändern 143

Netzwerkregel für ein Programm erstellen 143

Ausnahmen anpassen 144

Vererbung von Beschränkungen eines übergeordneten Prozesses 144

Regeln für Programme löschen 145

GRUPPENREGELN ÄNDERN

In der Grundeinstellung sind für die einzelnen Sicherheitsgruppen optimale Rechte für den Zugriff auf Computerressourcen vorgegeben. Sie können die vordefinierten Gruppenregeln ändern.

Gehen Sie folgendermaßen vor, um Gruppenregeln zu ändern:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.
4. Klicken Sie auf der rechten Fensterseite auf **Regeln konfigurieren**.
5. Wählen Sie im folgenden Fenster **Regeln für Programmgruppen** die entsprechende Gruppe aus.
6. Ändern Sie im folgenden Fenster auf der Registerkarte **Regeln** die Zugriffsrechte für die entsprechende Ressourcenkagetorie.

PROGRAMMREGELN ÄNDERN

Wenn ein Programm zum ersten Mal gestartet wird, ermittelt die Programmkontrolle seinen Status und weist es der entsprechenden Gruppe zu. Dann registriert die Komponente die Aktionen, die von diesem Programm im System ausgeführt werden können, und reguliert in Abhängigkeit von der Gruppe, zu der es gehört, seine Aktivität. Beim Zugriff eines Programms auf eine Ressource untersucht die Komponente, ob das Programm die erforderlichen Zugriffsrechte besitzt, und führt die von einer Regel vorgegebene Aktion aus. Sie können eine Regel ändern, die erstellt wurde, als der Status für das Programm ermittelt und es in die entsprechende Gruppe verschoben wurde.

Gehen Sie folgendermaßen vor, um eine Regel für ein Programm zu ändern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.

   Das Fenster **Computersicherheit** wird geöffnet.
2. Wählen Sie auf der linken Seite des Fensters den Abschnitt **Programmkontrolle**.
3. Klicken Sie im rechten Fensterbereich auf den Link **Programmaktivität**.
4. Wählen Sie im folgenden Fenster **Programmaktivität** in der Liste **Kategorie** die entsprechende Programmkategorie aus.
5. Führen Sie für das erforderliche Programm in der Spalte **Gruppe** einen Linksklick auf den Link mit dem Namen der Programmgruppe aus.
6. Wählen Sie im Kontextmenü den Punkt **Benutzerdefinierte Parameter**.
7. Ändern Sie im folgenden Fenster auf der Registerkarte **Regeln** die Zugriffsrechte für die entsprechende Ressourcenkagetorie.

NETZWERKREGEL FÜR EIN PROGRAMM ERSTELLEN

Falls der Zugriff eines Programms auf bestimmte Netzwerkdienste auf spezielle Weise verarbeitet werden soll, können Sie eine Netzwerkregel erstellen.

Gehen Sie folgendermaßen vor, um eine Regel zu erstellen, die die Netzwerkaktivität eines Programms reguliert:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.

   Das Fenster **Computersicherheit** wird geöffnet.
2. Wählen Sie auf der linken Seite des Fensters den Abschnitt **Programmkontrolle**.
3. Klicken Sie im rechten Fensterbereich auf den Link **Programmaktivität**.
4. Wählen Sie im folgenden Fenster **Programmaktivität** in der Liste **Kategorie** die entsprechende Programmkategorie aus.

5. Führen Sie für das erforderliche Programm in der Spalte **Gruppe** einen Linksklick auf den Link mit dem Namen der Programmgruppe aus.

6. Wählen Sie im Kontextmenü den Punkt **Benutzerdefinierte Parameter**.

7. Wählen Sie im folgenden Fenster auf der Registerkarte **Regeln** in der Dropdown-Liste die Kategorie **Netzwerkregeln** und klicken Sie auf den Link **Hinzufügen**.

8. Legen Sie im folgenden Fenster **Netzwerkregel** die Einstellungen für die Netzwerkregel fest.

9. Legen Sie die Priorität der neuen Regel fest, indem Sie sie mit Hilfe der Schaltflächen **Aufwärts** oder **Abwärts** in der Liste nach oben oder unten verschieben.

   Nachdem eine Regel erstellt wurde, können ihre Einstellungen geändert werden oder die Regel kann gelöscht werden. Dazu dienen die entsprechenden Schaltflächen im oberen Bereich der Registerkarte. Um eine Regel zu deaktivieren, entfernen Sie das Kontrollkästchen neben ihrem Namen.

AUSNAHMEN ANPASSEN

Wenn eine Regel für ein Programm erstellt wird, kontrolliert Kaspersky PURE standardmäßig alle Aktionen des Programms: Zugriff auf Dateien und Ordner, Zugriff auf die Ausführungsumgebung und Zugriff auf ein Netzwerk. Sie können bestimmte Aktionen von Programmen von der Untersuchung ausschließen.

Gehen Sie folgendermaßen vor, um die Aktionen eines Programms von der Untersuchung auszuschließen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.

   Das Fenster **Computersicherheit** wird geöffnet.

2. Wählen Sie auf der linken Seite des Fensters den Abschnitt **Programmkontrolle**.

3. Klicken Sie im rechten Fensterbereich auf den Link **Programmaktivität**.

4. Wählen Sie im folgenden Fenster **Programmaktivität** in der Liste **Kategorie** die entsprechende Programmkategorie aus.

5. Führen Sie für das erforderliche Programm in der Spalte **Gruppe** einen Linksklick auf den Link mit dem Namen der Programmgruppe aus.

6. Wählen Sie im Kontextmenü den Punkt **Benutzerdefinierte Parameter**.

7. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Ausnahmen** die Kontrollkästchen der auszuschließenden Aktionen. Wenn der Netzwerkverkehr eines Programms von der Untersuchung ausgeschlossen wird, passen Sie die zusätzlichen Parameter der Ausnahme an.

   Alle Ausnahmen, die in den Regeln für Programme erstellt wurden, stehen im Konfigurationsfenster für die Programmparameter im Abschnitt **Gefahren und Ausnahmen** zur Verfügung.

VERERBUNG VON BESCHRÄNKUNGEN EINES ÜBERGEORDNETEN PROZESSES

Als Initiator für den Start eines Programms kann entweder der Benutzer oder ein anderes laufendes Programm auftreten. Wenn ein anderes Programm als Initiator auftritt, entsteht eine Startfolge, die übergeordnete und untergeordnete Programme umfasst.

Wenn ein Programm versucht, Zugriff auf eine geschützte Ressource zu erhalten, analysiert die Programmkontrolle für alle übergeordneten Programmprozesse die Zugriffsrechte auf die Ressource. Dabei wird die Regel mit der minimalen Priorität ausgeführt: Beim Vergleich von Zugriffsrechten eines Programms und eines übergeordneten Prozesses werden auf die Programmaktivität die Zugriffsrechte mit der geringsten Priorität angewendet.

Priorität der Zugriffsrechte:

1. Erlauben Diese Zugriffsrechte besitzen die höchste Priorität.

2. Benutzer fragen.

3. Blockieren Diese Zugriffsrechte besitzen die niedrigste Priorität.

Dieser Mechanismus verhindert, dass vertrauenswürdige Programme von zweifelhaften Programmen oder von Programmen, die über beschränkte Rechte verfügen, dazu benutzt werden, privilegierte Aktionen auszuführen.

Wenn die Aktivität eines Programms blockiert wird, weil ein übergeordneter Prozess unzureichende Rechte besitzt, können Sie diese Rechte anpassen (s. Abschnitt "Programmregeln ändern" auf S. 143).

Das Ändern von Rechten eines übergeordneten Prozesses oder das Ausschalten des Vererbungsmechanismus sollte nur dann erfolgen, wenn Sie absolut sicher sind, dass die Aktivität des Prozesses keine Gefahr für das System darstellt!

Gehen Sie folgendermaßen vor, um die Vererbung von Beschränkungen eines übergeordneten Prozesses zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.

   Das Fenster **Computersicherheit** wird geöffnet.

2. Wählen Sie auf der linken Seite des Fensters den Abschnitt **Programmkontrolle**.

3. Klicken Sie im rechten Fensterbereich auf den Link **Programmaktivität**.

4. Wählen Sie im folgenden Fenster **Programmaktivität** in der Liste **Kategorie** die entsprechende Programmkategorie aus.

5. Führen Sie für das erforderliche Programm in der Spalte **Gruppe** einen Linksklick auf den Link mit dem Namen der Programmgruppe aus.

6. Wählen Sie im Kontextmenü den Punkt **Benutzerdefinierte Parameter**.

7. Deaktivieren Sie im folgenden Fenster auf der Registerkarte **Regeln** das Kontrollkästchen **Beschränkungen des übergeordneten Prozesses (Programms) übernehmen**.

REGELN FÜR PROGRAMME LÖSCHEN

Standardmäßig werden die Regeln für Programme, die innerhalb der letzten 60 Tage nicht gestartet wurden, automatisch gelöscht. Sie können die Speicherdauer der Regeln für nicht verwendete Programme ändern oder das automatische Löschen deaktivieren.

Gehen Sie folgendermaßen vor, um eine Speicherdauer für Programmregeln festzulegen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Fensterbereich auf den Link **Einstellungen**.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.

3. Aktivieren Sie für diese Komponente im Block **Erweitert** das Kontrollkästchen **Regeln für Programme löschen, wenn nicht gestartet seit** und geben Sie die entsprechende Anzahl der Tage an.

Gehen Sie folgendermaßen vor, um das automatische Löschen der Regeln für nicht verwendete Programme zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Fensterbereich auf den Link **Einstellungen**.

2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.

3. Deaktivieren Sie für die ausgewählte Komponente im Block **Erweitert** das Kontrollkästchen **Regeln für Programme löschen, wenn nicht gestartet seit**.

SCHUTZ FÜR BETRIEBSSYSTEMRESSOURCEN UND PERSÖNLICHE DATEN

Die Programmkontrolle verwaltet die Rechte von Programmen, die für das Ausführen von Aktionen mit diversen Ressourcenkategorien des Betriebssystems und der persönlichen Daten gelten.

Die Kaspersky-Lab-Experten haben Kategorien für geschützte Ressourcen vordefiniert. Diese Liste kann nicht verändert werden. Sie können dieser Liste aber benutzerdefinierte Kategorien und / oder einzelne Ressourcen hinzufügen, und die Kontrolle bestimmter Ressourcen deaktivieren.

- *Gehen Sie folgendermaßen vor, um geschützte persönliche Daten hinzuzufügen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Fensterbereich auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.
3. Klicken Sie für die ausgewählte Komponente auf **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Persönliche Daten** in der Dropdown-Liste **Kategorie** die entsprechende Kategorie für persönliche Daten und öffnen Sie mit dem Link **Hinzufügen** das Fenster, in dem die Ressourcen hinzugefügt werden.
5. Klicken Sie im folgenden Fenster **Benutzerressource** auf **Durchsuchen** und geben Sie in Abhängigkeit von der ausgewählten Ressource die notwendigen Daten an:

Nachdem eine Ressource hinzugefügt wurde, kann sie geändert oder gelöscht werden. Dazu dienen die entsprechenden Schaltflächen im oberen Bereich der Registerkarte. Um eine Ressource oder eine Kategorie von der Kontrolle auszuschließen, deaktivieren Sie das entsprechende Kontrollkästchen.

- *Gehen Sie folgendermaßen vor, um eine Kategorie für geschützte persönliche Daten zu erstellen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Fensterbereich auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.
3. Klicken Sie für die ausgewählte Komponente auf **Einstellungen**.
4. Öffnen Sie im folgenden Fenster auf der Registerkarte **Persönliche Daten** mit dem Link **Kategorie hinzufügen** das Fenster, in dem Ressourcen hinzugefügt werden können..
5. Geben Sie im folgenden Fenster **Kategorie für Benutzerressourcen** einen Namen für die neue Ressourcenkategorie ein.

- *Gehen Sie folgendermaßen vor, um geschützte Parameter und Ressourcen des Betriebssystems hinzuzufügen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Fensterbereich auf den Link **Einstellungen**.
2. Wählen Sie im folgenden Fenster im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.
3. Klicken Sie für die ausgewählte Komponente auf **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Betriebssystem** in der Dropdown-Liste **Kategorie** die entsprechende Kategorie für die Betriebssystemobjekte und öffnen Sie mit dem Link **Hinzufügen** das Fenster, in dem die Ressourcen hinzugefügt werden.

Nachdem eine Ressource hinzugefügt wurde, kann sie geändert oder gelöscht werden. Dazu dienen die entsprechenden Schaltflächen im oberen Bereich der Registerkarte. Um eine Ressource oder eine Kategorie von der Kontrolle auszuschließen, deaktivieren Sie das entsprechende Kontrollkästchen.

PROAKTIVER SCHUTZ

Der Proaktive Schutz bietet Schutz vor neuen Bedrohungen, über die in den Datenbanken von Kaspersky PURE keine Informationen vorhanden sind.

Die präventiven Technologien, auf denen der Proaktive Schutz beruht, erlauben es, einen Zeitverlust zu vermeiden und eine neue Bedrohung zu neutralisieren, bevor sie auf Ihrem Computer Schaden verursachen kann. Im Unterschied zu den reaktiven Technologien, bei denen die Analyse auf Basis von Einträgen der Datenbanken von Kaspersky PURE erfolgt, identifizieren die Präventivtechnologien eine neue Bedrohung auf Ihrem Computer nach den Aktionsfolgen, die von einem bestimmten Programm ausgeführt werden. Wenn aufgrund der Aktivitätsanalyse die Aktionsfolge eines Programms als verdächtig eingestuft wird, sperrt Kaspersky PURE ihre Aktivität.

Werden beispielsweise Aktionen erkannt, bei denen sich ein bestimmtes Programm selbst in eine Netzwerkressource, in den Autostart-Ordner und in die Systemregistrierung kopiert, so handelt es sich mit hoher Wahrscheinlichkeit um einen Wurm. Als gefährliche Aktionsfolgen gelten auch Änderungsversuche der HOSTS-Datei, versteckte Treiberinstallation u.a. Sie können für eine bestimmte gefährliche Aktivität die Kontrolle deaktivieren oder die entsprechenden Kontrollregeln ändern (s. S. 148).

Im Unterschied zur Programmkontrolle reagiert der Proaktive Schutz genau auf bestimmte Aktionsfolgen eines Programms. Die Aktivitätsanalyse erstreckt sich auf alle Programme, einschließlich der Programme, die von der Komponente Programmkontrolle der Gruppe **Vertrauenswürdig** zugeordnet wurden (auf S. 138).

Sie können für den proaktiven Schutz eine Gruppe mit vertrauenswürdigen Programmen anlegen (s. S. 148). Über die Aktivität solcher Programme werden keine Meldungen angezeigt.

Wenn ein Computer mit den Betriebssystemen Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64, Microsoft Windows 7 oder Microsoft Windows 7 x64 arbeitet, werden nicht alle Ereignisse kontrolliert. Dies hängt mit Besonderheiten der genannten Betriebssysteme zusammen. Nicht in vollem Umfang kontrolliert werden beispielsweise das Senden von Daten über vertrauenswürdige Programme und verdächtige Aktivität im System.

IN DIESEM ABSCHNITT

Proaktiven Schutz aktivieren und deaktivieren 147

Gruppe mit vertrauenswürdigen Programmen erstellen 148

Liste der gefährlichen Aktivität verwenden 148

Kontrollregel für gefährliche Aktivität ändern 148

Rollback von Aktionen eines schädlichen Programms 149

PROAKTIVEN SCHUTZ AKTIVIEREN UND DEAKTIVIEREN

Der Proaktive Schutz ist standardmäßig aktiviert und arbeitet im optimalen Modus. Sie können den Proaktiven Schutz bei Bedarf deaktivieren.

Gehen Sie folgendermaßen vor, um den Proaktiven Schutz zu aktivieren oder zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite unter **Schutz-Center** die Komponente **Proaktiver Schutz**.

4. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Proaktiven Schutz aktivieren**, um die Komponente auszuschalten. Aktivieren Sie dieses Kontrollkästchen, um die Komponente einzuschalten.

GRUPPE MIT VERTRAUENSWÜRDIGEN PROGRAMMEN ERSTELLEN

Programme, die von der Komponente Programmkontrolle den Status **Vertrauenswürdig** erhalten, stellen keine Gefahr für das System dar. Trotzdem wird ihre Aktivität auch von der Komponente Proaktiver Schutz kontrolliert.

Sie können eine Gruppe mit vertrauenswürdigen Programmen erstellen, deren Aktivität nicht vom Proaktiven Schutz überwacht werden soll. Als vertrauenswürdig gelten standardmäßig jene Programme, die eine verifizierte digitale Signatur besitzen oder in der Datenbank von Kaspersky Security Network enthalten sind.

Gehen Sie folgendermaßen vor, um die Einstellungen zu ändern, die für das Anlegen einer Gruppe für vertrauenswürdige Programme gelten:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite unter **Schutz-Center** die Komponente **Proaktiver Schutz**.
4. Aktivieren Sie auf der rechten Fensterseite im Block **Vertrauenswürdige Programme** die Kontrollkästchen für die entsprechenden Parameter.

LISTE DER GEFÄHRLICHEN AKTIVITÄT VERWENDEN

Die Liste der Aktionen, die als gefährliche Aktivität gelten, kann nicht verändert werden. Dabei können Sie die Kontrolle bestimmter Typen gefährlicher Aktivität deaktivieren.

Gehen Sie folgendermaßen vor, um die Kontrolle bestimmter Typen gefährlicher Aktivität zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite unter **Schutz-Center** die Komponente **Proaktiver Schutz**.
4. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.
5. Deaktivieren Sie im folgenden Fenster **Proaktiver Schutz** das Kontrollkästchen neben dem Namen des Aktivitätstyps, der nicht kontrolliert werden soll.

KONTROLLREGEL FÜR GEFÄHRLICHE AKTIVITÄT ÄNDERN

Aktionen für Programme, deren Aktivität als gefährlich klassifiziert wurde, können nicht geändert werden. Sie können folgende Aktionen ausführen:

- die Kontrolle bestimmter Typen gefährlicher Aktivität deaktivieren (s. S. 148).
- Liste von Ausnahmen erstellen, indem Sie die Programme festlegen, deren Aktivität Sie nicht für gefährlich halten.
- Regel ändern, nach welcher der Proaktive Schutz beim Fund einer gefährlichen Aktivität vorgeht.

Gehen Sie folgendermaßen vor, um eine Regel zu ändern:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie auf der linken Fensterseite unter **Schutz-Center** die Komponente **Proaktiver Schutz**.

4. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

5. Wählen Sie im folgenden Fenster **Proaktiver Schutz** in der Spalte **Ereignis** das Ereignis, für das die Regel geändert werden soll.

6. Legen Sie für das gewählte Ereignis mit Hilfe der Links im Block **Regelbeschreibung** die entsprechenden Parameter fest: Beispielsweise:

   a. Klicken Sie auf den Link mit der geltenden Aktion und wählen Sie im folgenden Fenster **Aktion wählen** die entsprechende Aktion.

   b. Klicken Sie auf den Link für das geltende Intervall (Es wird nicht für alle Aktivitätsarten ein Intervall angegeben) und legen Sie im folgenden Fenster **Versteckte Prozesse erkennen** ein Intervall fest, in dem die Suche nach versteckten Prozessen erfolgen soll.

   c. Klicken Sie auf den Link **Ein / Aus**, um festzulegen, ob die ausgeführte Operation protokolliert werden soll.

ROLLBACK VON AKTIONEN EINES SCHÄDLICHEN PROGRAMMS

Der Proaktive Schutz erlaubt es, schädliche Aktivitäten im System rückgängig zu machen.

Wenn Kaspersky PURE im automatischen Modus arbeitet, werden die Aktionen eines schädlichen Programms automatisch rückgängig gemacht, wenn von der Komponente Proaktiver Schutz eine schädliche Aktivität erkannt wird. Im interaktiven Modus (s. S. 61) können Sie die Aktion ändern, die beim Erkennen einer schädlichen Aktivität ausgeführt werden soll.

Das Rollback der Aktionen eines schädlichen Programms betrifft eine begrenzte Auswahl von Daten. Es hat keinerlei negativen Einfluss auf die Funktion des Betriebssystems und führt nicht zu Datenverlust auf Ihrem Computer.

Gehen Sie folgendermaßen vor, um ein Rollback von Aktionen, die von einem schädlichen Programm ausgeführt wurden, anzupassen:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie auf der linken Fensterseite unter **Schutz-Center** die Komponente **Proaktiver Schutz**.

4. Wählen Sie im rechten Fensterbereich im Block **Erweitert** die erforderliche Reaktion auf Aktionen eines schädlichen Programms aus.

NETZWERKSCHUTZ

Unterschiedliche Schutzkomponenten, Tools und Konfigurationen von Kaspersky PURE bieten Ihnen Sicherheit bei der Arbeit in einem Netzwerk.

Die folgenden Abschnitte informieren ausführlich über folgende Themen: Funktionsprinzipien und Einstellungen der Firewall und des Schutzes vor Netzwerkangriffen, Netzwerkmonitor, Untersuchung von geschützten Verbindungen, Proxyserver-Einstellungen, Kontrolle von Netzwerkports.

IN DIESEM ABSCHNITT

Firewall 151

Schutz vor Netzwerkangriffen 154

Untersuchung geschützter Verbindungen 157

Netzwerkmonitor 159

Proxyserver-Einstellungen 159

Liste der zu kontrollierenden Ports erstellen 160

FIREWALL

Firewall gewährleistet Sicherheit bei der in lokalen Netzwerken und im Internet.

Die Komponente filtert die gesamte Netzwerkaktivität in Übereinstimmung mit den Netzwerkregeln der Programmkontrolle. Eine Netzwerkregel besteht aus einer Aktion, die von der Firewall ausgeführt wird, wenn ein Verbindungsversuch mit einem bestimmten Status erkannt wird. Jeder Netzwerkverbindung wird ein Status zugewiesen, der durch bestimmte Parameter definiert wird: Richtung und Protokoll für die Datenübertragung, Adressen und Ports, mit denen die Verbindung erfolgt.

Die Firewall analysiert die Parameter der Netzwerke, die Sie mit Ihrem Computer verbinden. Wenn das Programm im interaktiven Funktionsmodus arbeitet, fragt die Firewall Sie bei der ersten Verbindung nach dem Status des verbundenen Netzwerks. Wenn der interaktive Funktionsmodus deaktiviert wurde, ermittelt die Firewall den Status, wozu Netzwerktyp, Adressenbereich und anderen Merkmale verwendet werden. Sie können den Status einer Netzwerkverbindung manuell ändern.

IN DIESEM ABSCHNITT

Firewall aktivieren und deaktivieren 151

Netzwerkstatus ändern 151

Adressenbereich eines Netzwerks erweitern 152

Arbeit mit den Firewall-Regeln 152

Benachrichtigungen über Veränderungen eines Netzwerks anpassen 154

Erweiterte Einstellungen für die Firewall 154

FIREWALL AKTIVIEREN UND DEAKTIVIEREN

Firewall ist standardmäßig aktiviert und arbeitet im optimalen Modus. Bei Bedarf können Sie die Firewall deaktivieren.

Gehen Sie folgendermaßen vor, um die Firewall zu aktivieren oder zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Firewall**.
4. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Firewall aktivieren**, um die Komponente auszuschalten. Aktivieren Sie dieses Kontrollkästchen, um die Komponente einzuschalten.

NETZWERKSTATUS ÄNDERN

Vom Status der Netzwerkverbindung hängt ab, welche Filterregeln für die Netzwerkaktivität dieser Verbindung zur Anwendung kommen. Bei Bedarf können Sie den Netzwerkstatus ändern.

Gehen Sie folgendermaßen vor, um den Status einer Netzwerkverbindung zu ändern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Fensterbereich auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Firewall**.
3. Klicken Sie für die ausgewählte Komponente auf **Einstellungen**.

4. Wählen Sie im folgenden Fenster auf der Registerkarte **Netzwerke** eine aktive Netzwerkverbindung aus und klicken Sie auf den Link **Ändern**.

5. Wählen Sie im folgenden Fenster auf der Registerkarte **Eigenschaften** den erforderlichen Status der Dropdown-Liste.

ADRESSENBEREICH EINES NETZWERKS ERWEITERN

Jedem Netzwerk entsprechen ein oder mehrere IP-Adressenbereiche. Wenn Sie eine Verbindung mit einem Netzwerk herstellen, auf dessen Subnetze über einen Router zugegriffen wird, können Sie die darüber verfügbaren Subnetze manuell hinzufügen.

Beispiel: Sie stellen eine Verbindung zu dem Netzwerk eines Büros Ihrer Firma her und möchten, dass die Filterregeln für das Büro, mit dem die Direktverbindung erfolgt, und für die über dieses Netzwerk erreichbaren Büros, einheitlich sind.

Erkundigen Sie sich beim Netzwerkadministrator nach den Adressenbereichen dieser Büros und fügen Sie diese hinzu.

Gehen Sie folgendermaßen vor, um den Adressenbereichs eines Netzwerks zu erweitern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Fensterbereich auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Firewall**.

3. Klicken Sie für die ausgewählte Komponente auf **Einstellungen**.

4. Wählen Sie im folgenden Fenster auf der Registerkarte Netzwerke eine aktive Netzwerkverbindung aus und klicken Sie auf den Link **Ändern**.

5. Klicken Sie im folgenden Fenster auf der Registerkarte **Eigenschaften** im Block **Zusätzliche Subnetze** auf den Link **Hinzufügen**.

6. Legen Sie im folgenden Fenster **IP-Adresse** eine IP-Adresse oder eine Adressenmaske fest.

ARBEIT MIT DEN FIREWALL-REGELN

Die Firewall arbeitet mit zwei Arten von Regeln:

- *Paketregeln.* Dienen zur Definition von Beschränkungen für die Pakete, wobei das Programm keine Rolle spielt. Solche Regeln beziehen sich meistens auf die eingehende Netzwerkaktivität bestimmter Ports mit den Protokollen TCP und UDP und regulieren die Filterung von ICMP-Nachrichten.

- *Programmregeln*. Dienen zur Definition von Beschränkungen für die Netzwerkaktivität eines konkreten Programms. Solche Regeln erlauben es, die Aktivitätsfilterung genau anzupassen, wenn beispielsweise ein bestimmter Typ von Netzwerkverbindungen für konkrete Programme verboten, für andere aber erlaubt werden soll.

Paketregeln besitzen eine höhere Priorität als Programmregeln. Wenn für eine Art der Netzwerkaktivität gleichzeitig Paketregeln und Programmregeln vorhanden sind, wird diese Netzwerkaktivität nach den Paketregeln verarbeitet. Außerdem können Sie für jede Regel eine Ausführungspriorität festlegen.

PAKETREGEL ERSTELLEN

Paketregeln bestehen aus einer Kombination von Bedingungen und Aktionen, die unter bestimmten Bedingungen mit Paketen ausgeführt werden.

Wenn Sie Paketregeln erstellen, beachten Sie, dass diese eine höhere Priorität besitzen als Regeln für Programme.

Gehen Sie folgendermaßen vor, um eine neue Paketregel zu erstellen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Fensterbereich auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Firewall**.

3. Klicken Sie für die ausgewählte Komponente auf **Einstellungen**.

4. Wählen Sie im folgenden Fenster auf der Registerkarte **Filterregeln** den Block **Paketregeln** aus und klicken Sie auf den Link **Hinzufügen**.

5. Legen Sie im folgenden Fenster **Netzwerkregel** die entsprechenden Parameter fest und klicken Sie auf **OK**.

6. Legen Sie die Priorität der neuen Regel fest, indem Sie sie mit Hilfe der Links **Aufwärts** und **Abwärts** in der Liste nach oben oder unten verschieben.

   Nachdem eine Regel erstellt wurde, können ihre Einstellungen geändert werden oder die Regel kann gelöscht werden. Dazu dienen die entsprechenden Links im unteren Bereich der Registerkarte. Um eine Regel zu deaktivieren, entfernen Sie das Kontrollkästchen neben ihrem Namen.

GRUPPENREGELN ÄNDERN

Analog zur Komponente Programmkontrolle (s. S. 138) verwendet die Firewall zur Filterung der Netzwerkaktivität standardmäßig die Regeln der Gruppe, in die das Programm verschoben wurde.

Die Netzwerkregeln für die Sicherheitsgruppen legen fest, welche Rechte die Programme, die dieser Gruppe angehören, für den Zugriff auf unterschiedliche Netzwerke besitzen. Sie können die vordefinierten Netzwerkregeln für eine Gruppe ändern.

Gehen Sie folgendermaßen vor, um eine Netzwerkregel für eine Gruppe zu ändern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Fensterbereich auf den Link **Einstellungen**.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Firewall**.

3. Klicken Sie für die ausgewählte Komponente auf **Regeln anpassen**.

4. Wählen Sie im folgenden Fenster eine Gruppe aus, öffnen Sie durch Rechtsklick das Kontextmenü für das Netzwerk und wählen Sie dort den entsprechenden Wert aus: **Erlauben**, **Verbieten** oder **Aktion erfragen**.

PROGRAMMREGELN ÄNDERN

Sie können Netzwerkregeln für bestimmte Programme erstellen. Netzwerkregeln für ein Programm besitzen eine höhere Priorität als Netzwerkregeln für eine Gruppe.

Bei Bedarf können Sie mit der Komponente Programmkontrolle Netzwerkregeln (s. S. 143) für Programme erstellen.

Gehen Sie folgendermaßen vor, um eine Regel für ein Programm zu erstellen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Fensterbereich auf den Link **Einstellungen** im oberen Bereich des Fensters.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Firewall**.

3. Klicken Sie für die ausgewählte Komponente auf **Einstellungen**.

4. Wählen Sie im folgenden Fenster auf der Registerkarte **Filterregeln** eine Regelgruppe für ein Programm aus und klicken Sie auf den Link **Hinzufügen**.

5. Legen Sie im folgenden Fenster **Netzwerkregel** die Einstellungen für die Netzwerkregel fest.

6. Legen Sie die Priorität der neuen Regel fest, indem Sie sie mit Hilfe der Links **Aufwärts** und **Abwärts** in der Liste nach oben oder unten verschieben.

   Nachdem eine Regel erstellt wurde, können ihre Einstellungen geändert werden oder die Regel kann gelöscht werden. Dazu dienen die entsprechenden Links im unteren Bereich der Registerkarte. Um eine Regel zu deaktivieren, entfernen Sie das Kontrollkästchen neben ihrem Namen.

BENACHRICHTIGUNGEN ÜBER VERÄNDERUNGEN EINES NETZWERKS ANPASSEN

Die Parameter von Netzwerkverbindungen können sich im Verlauf der Arbeit ändern. Sie können sich über Einstellungsveränderungen informieren lassen:

Gehen Sie folgendermaßen vor, um die Benachrichtigungen über Veränderungen der Parameter einer Netzwerkverbindung anzupassen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Fensterbereich auf den Link **Einstellungen**.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Firewall**.
3. Klicken Sie für die ausgewählte Komponente auf **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Netzwerke** eine aktive Netzwerkverbindung aus und klicken Sie auf den Link **Ändern**.
5. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Erweitert** die Kontrollkästchen für die Ereignisse, über die eine Meldung erfolgen soll.

ERWEITERTE EINSTELLUNGEN FÜR DIE FIREWALL

Sie können die Arbeit der Firewall zusätzlich anpassen, d.h. den aktiven FTP-Modus zulassen, eine Verbindung blockieren, wenn keine Aktionsanfrage möglich ist (wenn das Programminterface nicht geladen ist), und festlegen, dass die Firewall erst beendet wird, wenn das System vollständig heruntergefahren wird.

In der Grundeinstellung sind diese Parameter deaktiviert.

Gehen Sie folgendermaßen vor, um zusätzliche Parameter für die Firewall festzulegen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Fensterbereich auf den Link **Einstellungen** im oberen Bereich des Fensters.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Firewall**.
3. Klicken Sie für die ausgewählte Komponente auf **Einstellungen**.
4. Klicken Sie im folgenden Fenster auf der Registerkarte **Filterregeln** auf **Erweitert**.
5. Aktivieren / deaktivieren Sie im folgenden Fenster **Erweitert** die Kontrollkästchen für die entsprechenden Parameter.

SCHUTZ VOR NETZWERKANGRIFFEN

Der Schutz vor Netzwerkangriffen überwacht den eingehenden Datenverkehr auf für Netzwerkangriffe charakteristische Aktivität. Wenn ein Angriffsversuch auf Ihren Computer erkannt wird, blockiert Kaspersky PURE jede Art von Netzwerkaktivität des angreifenden Computers im Hinblick auf Ihrem Computer.

In der Grundeinstellung dauert die Blockade eine Stunde. Sie können die Einstellungen für das Blockieren ändern (s. S. 156). Auf dem Bildschirm erscheint eine Meldung über den Angriffsversuch. Die Meldung enthält Informationen über den angreifenden Computer. Beschreibungen der momentan bekannten Netzwerkangriffe (s. Abschnitt "Arten der erkennbaren Netzwerkangriffe" auf S. 155) und entsprechende Abwehrmethoden sind in den Datenbanken von Kaspersky PURE enthalten. Die Liste der Angriffe, die der Schutz vor Netzwerkangriffen erkennt, wird im Rahmen des Updates (s. Abschnitt "Update" auf S. 93) der Datenbanken aktualisiert.

IN DIESEM ABSCHNITT

Arten der erkennbaren Netzwerkangriffe 155

Schutz vor Netzwerkangriffen aktivieren und deaktivieren 156

Parameter für das Blockieren ändern 156

ARTEN DER ERKENNBAREN NETZWERKANGRIFFE

Heutzutage existiert einen Vielzahl unterschiedlicher Arten von Netzwerkangriffen. Diese Angriffe nutzen sowohl Schwachstellen des Betriebssystems, als auch installierte System- und Anwendungsprogramme aus.

Um rechtzeitig für die Sicherheit des Computers zu sorgen, ist es wichtig zu wissen, welche Arten von Netzwerkangriffen ihm drohen können. Die bekannten Netzwerkangriffe lassen sich bedingt in drei große Gruppen unterteilen:

- *Scannen von Ports* – Diese Bedrohungsart stellt getrennt betrachtet keinen Angriff dar, sondern geht diesem voraus, weil sie eine der effektivsten Methoden ist, Informationen über einen Remote-Computer zu erhalten. Die Methode besteht darin, die von Netzwerkdiensten auf dem angegriffenen Computer verwendeten UDP/TCP-Ports zu scannen, um deren Status (geschlossene oder offene Ports) zu ermitteln.

  Das Scannen von Ports gibt Aufschluss darüber, welche Angriffstypen für ein bestimmtes System am meisten Erfolg versprechen. Außerdem verleihen die aus dem Scannen resultierenden Informationen ("Abdruck" des Systems) dem Angreifer eine Vorstellung vom Typ des Betriebssystems auf dem entfernten Computer. Dadurch lässt sich die Art der relevanten Angriffe weiter einkreisen und damit die zum Ausführen der Angriffe notwendige Zeit verkürzen. Außerdem können die für das Betriebssystem spezifischen Sicherheitslücken ausgenutzt werden.

- *DoS-Angriffe* oder Angriffe, die zur Dienstverweigerung führen Das Ziel dieser Angriffe besteht darin, die Instabilität des angegriffenen Systems hervorzurufen oder es vollständig außer Gefecht zu setzen. Aufgrund solcher Angriffe können die betroffenen Informationsressourcen unzugänglich werden (z.B. gestörter Internetzugriff).

  Es gibt zwei Haupttypen von DoS-Angriffen:

  - Es werden spezielle Pakete an den angegriffenen Computer geschickt, die dieser nicht erwartet. Die Folge ist eine Überlastung oder ein Systemabsturz.

  - An den angegriffenen Computer wird innerhalb eines kurzen Zeitraums eine große Anzahl von Paketen geschickt, die dieser Computer nicht verarbeiten kann. Als Folge erschöpfen die Systemressourcen.

  Die folgenden Angriffe bieten gute Beispiele für diese Gruppe:

  - Der Angriff *Ping of death* besteht im Senden eines ICMP-Pakets, dessen Größe den zulässigen Wert von 64 KB überschreitet. Dieser Angriff kann zum Absturz bestimmter Betriebssysteme führen.

  - Bei dem Angriff *Land* wird an einen offenen Port Ihres Computers eine Anfrage auf Verbindungsherstellung mit sich selbst gesendet. Der Angriff führt im angegriffenen Computer zu einer Endlosschleife, was eine stark erhöhte Prozessorbelastung zur Folge hat und bei bestimmten Betriebssystemen zum Absturz führen kann.

  - Bei dem Angriff *ICMP Flood* wird eine große Anzahl von ICMP-Paketen an Ihren Computer gesendet Da der Computer auf jedes eintreffende Paket reagieren muss, kommt es zu einer erheblichen Erhöhung der Prozessorauslastung.

  - Bei dem Angriff *SYN Flood* wird eine große Menge von Verbindungsanfragen an Ihren Computer gesendet. Das System reserviert für jede dieser Verbindungen bestimmte Ressourcen, wodurch es seine Ressourcen vollständig verbraucht und nicht mehr auf andere Verbindungsversuche reagiert.

- *Angriffe zur "Übernahme"* - Diese Angriffe zielen auf die "Übernahme" des Systems ab. Dies ist der gefährlichste Angriffstyp, weil das System bei erfolgreichem Angriff dem Angreifer gegenüber vollkommen wehrlos ist.

  Dieser Angriff wird benutzt, um von einem Remote-Computer vertrauliche Informationen zu stehlen (beispielsweise Kreditkartennummern und Kennwörter). Ein weiteres Ziel kann darin bestehen, sich im System einzunisten, um später die Rechnerressourcen für die Zwecke des Angreifers zu nutzen (das angegriffene System wird in einem Zombie-Netzwerk oder als "Brückenkopf" für neue Angriffe verwendet).

  Zu dieser Gruppe gehört eine große Anzahl von Angriffen. Sie lassen sich abhängig von dem Betriebssystem, das auf einem Computer installiert ist, in drei Kategorien unterteilen: Angriffe auf Microsoft Windows-Systeme, Angriffe auf Unix-Systeme und eine allgemeine Gruppe für Netzwerkdienste, die in beiden Betriebssystemen verwendet werden.

  Die meistverbreiteten Arten von Angriffen, die auf Netzwerkdienste eines Betriebssystems zugreifen, sind:

  - *Angriffe mit dem Ziel des Pufferüberlaufs*. Ein Pufferüberlauf tritt durch fehlende (oder unzureichende) Kontrolle bei der Arbeit mit Daten-Arrays auf. Dieser Typ von Schwachstellen gehört zu den ältesten und lässt sich am leichtesten von Angreifern ausnutzen.

  - *Angriffe, die auf Fehlern in Formatzeilen beruhen*. Formatzeilenfehler treten auf, weil die Eingabeparameter von Formatfunktionen des Typs *printf(), fprintf(), scanf()* und anderer Standardbibliotheken der Sprache C unzureichend kontrolliert werden. Wenn diese Sicherheitslücke in einem Programm vorhanden ist, kann ein Angreifer die vollständige Kontrolle über das System übernehmen, wenn es ihm gelingt, speziell erstellte Anfragen zu senden.

    Wenn solche Schwachstellen auf dem Benutzercomputer vorhanden sind, werden sie vom Detektionssystem für Angriffe in den gebräuchlichsten Netzwerkdiensten (FTP, POP3, IMAP) automatisch analysiert und ihre Verwendung wird verhindert.

  - *Angriffe, die sich auf das Betriebssystem Microsoft Windows richten,* beruhen auf der Verwendung von Sicherheitslücken der auf einem Computer installierten Software (beispielsweise solcher Programme wie Microsoft SQL Server, Microsoft Internet Explorer, Messenger, sowie Systemkomponenten, die über ein Netzwerk erreichbar sind: DCom, SMB, Wins, LSASS, IIS5).

  Als weiterer häufig anzutreffender Typ von Übernahmeangriffen lässt sich die Verwendung unterschiedlicher Arten von schädlichen Skripts nennen. Dazu zählen auch Skripts, die von Microsoft Internet Explorer verarbeitet werden, sowie die Variationen des Helkern-Wurms. Bei einem Helkern-Angriff werden spezielle UDP-Pakete mit ausführbarem schädlichem Code an einen entfernten Computer gesendet.

SCHUTZ VOR NETZWERKANGRIFFEN AKTIVIEREN UND DEAKTIVIEREN

Der Schutz vor Netzwerkangriffen ist standardmäßig aktiviert und arbeitet im optimalen Modus. Bei Bedarf können Sie den Schutz vor Netzwerkangriffen deaktivieren.

Gehen Sie folgendermaßen vor, um den Schutz vor Netzwerkangriffen zu aktivieren oder zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite unter **Schutz-Center** die Komponente **Schutz vor Netzwerkangriffen**.
4. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Schutz vor Netzwerkangriffen aktivieren**, um die Komponente auszuschalten. Aktivieren Sie dieses Kontrollkästchen, um die Komponente einzuschalten.

PARAMETER FÜR DAS BLOCKIEREN ÄNDERN

In der Grundeinstellung blockiert der Schutz vor Netzwerkangriffen die Aktivität eines angreifenden Computers für eine Stunde. Sie können das Blockieren für einen bestimmten Computer aufheben oder die Sperrdauer ändern.

Gehen Sie folgendermaßen vor, um den Zeitraum, für den ein angreifender Computer gesperrt werden soll, zu ändern:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite unter **Schutz-Center** die Komponente **Schutz vor Netzwerkangriffen**.
4. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Angreifenden Computer zur Sperrliste hinzufügen für** und legen Sie eine Sperrdauer fest.

Gehen Sie folgendermaßen vor, um einen angreifenden Computer freizugeben:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.

   Das Fenster **Computersicherheit** wird geöffnet.
2. Wählen Sie auf der linken Fensterseite **Schutz-Center**.
3. Klicken Sie im rechten Fensterbereich im Abschnitt **Arbeit im Netzwerk** auf den Link **Netzwerkmonitor**, um das Fenster **Netzwerkmonitor** zu öffnen.
4. Wählen Sie auf der Registerkarte **Blockierte Computer** einen blockierten Computer aus und geben Sie diesen mit dem Link **Freigeben** frei.

UNTERSUCHUNG GESCHÜTZTER VERBINDUNGEN

Eine Verbindung unter Verwendung des SSL/TLS-Protokolls bietet den Schutz des Kommunikationskanals im Internet. Das des SSL/TLS-Protokoll erlaubt die Identifikation der am Datenaustausch beteiligten Partner. Dazu dienen elektronische Zertifikate. Außerdem werden die übertragenen Daten verschlüsselt und beim Übertragungsvorgang wird die Datenintegrität gewährleistet.

Diese Besonderheiten des Protokolls werden aber von Angreifern zur Verbreitung schädlicher Programme benutzt, weil die meisten Antiviren-Produkte den SSL/TLS-Verkehr nicht untersuchen.

Die Untersuchung von geschützten Verbindungen wird in Kaspersky PURE mit Hilfe eines Zertifikats von Kaspersky Lab realisiert.

Wenn bei der Verbindung mit einem Server ein inkorrektes Zertifikat gefunden wird (wenn es z.B. von einem ein Angreifer ausgetauscht wurde), erscheint auf dem Bildschirm eine Meldung, in der Sie das Zertifikat akzeptieren oder ablehnen.

Wenn Sie sicher sind, dass die Verbindung mit einer Webseite trotz des inkorrekten Zertifikats immer ungefährlich ist, können Sie die Webseite in die Liste der vertrauenswürdigen Adressen aufnehmen. Kaspersky PURE wird verschlüsselte Verbindungen mit dieser Webseite danach nicht mehr untersuchen.

Gehen Sie folgendermaßen vor, um die Untersuchung geschützter Verbindungen zu aktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite unter **Schutz-Center** den Abschnitt **Netzwerk**.
4. Aktivieren Sie im rechten Fensterbereich das Kontrollkästchen **Geschützte Verbindungen untersuchen** und klicken Sie auf **Zertifikat installieren**.
5. Klicken Sie im folgenden Fenster auf **Zertifikat installieren**. Es wird ein Assistent gestartet, der Sie bei der Installation eines Zertifikats unterstützt.

Die automatische Installation eines Zertifikats erfolgt nur bei der Arbeit mit dem Browser Microsoft Internet Explorer. Zur Untersuchung von geschützten Verbindungen in den Browsern Mozilla Firefox und Opera muss das Kaspersky-Lab-Zertifikat manuell installiert werden.

UNTERSUCHUNG GESCHÜTZTER VERBINDUNGEN IN MOZILLA FIREFOX

Der Browser Mozilla Firefox verwendet nicht den Zertifikatsspeicher von Microsoft Windows. Bei der Verwendung von Firefox ist es zur Untersuchung von SSL-Verbindungen erforderlich, das Kaspersky-Lab-Zertifikat manuell zu installieren.

Gehen Sie folgendermaßen vor, um das Kaspersky-Lab-Zertifikat zu installieren:

1. Wählen Sie im Menü des Browsers den Punkt **Tools** → **Einstellungen**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Erweitert**.
3. Wählen Sie im Block **Zertifikate** die Registerkarte **Sicherheit** und klicken Sie auf **Zertifikate anzeigen**.
4. Wählen Sie im folgenden Fenster die Registerkarte **Zertifizierungsstellen** und klicken Sie auf **Importieren**.
5. Wählen Sie im folgenden Fenster die Datei des Kaspersky-Lab-Zertifikats. Pfad der Datei des Kaspersky-Lab-Zertifikats: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.
6. Aktivieren Sie im folgenden Fenster die Kontrollkästchen der Aktionen, für deren Untersuchung das installierte Zertifikat verwendet werden soll. Anzeige von Informationen zu dem Zertifikat dient die Schaltfläche **Ansicht**.

Gehen Sie folgendermaßen vor, um das Kaspersky-Lab-Zertifikat für Mozilla Firefox Version 3.x zu installieren:

1. Wählen Sie im Menü des Browsers den Punkt **Tools** → **Einstellungen**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Erweitert**.
3. Klicken Sie auf der Registerkarte **Verschlüsselung** auf **Zertifikate anzeigen**.
4. Wählen Sie im folgenden Fenster die Registerkarte **Zertifizierungsstellen** und klicken Sie auf **Importieren**.
5. Wählen Sie im folgenden Fenster die Datei des Kaspersky-Lab-Zertifikats. Pfad der Datei des Kaspersky-Lab-Zertifikats: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.
6. Aktivieren Sie im folgenden Fenster die Kontrollkästchen der Aktionen, für deren Untersuchung das installierte Zertifikat verwendet werden soll. Anzeige von Informationen zu dem Zertifikat dient die Schaltfläche **Anzeigen**.

Wenn Ihr Computer mit dem Betriebssystem Microsoft Windows Vista arbeitet, lautet der Pfad der Zertifikatsdatei von Kaspersky Lab: *%AllUsersProfile%\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

UNTERSUCHUNG GESCHÜTZTER VERBINDUNGEN IN OPERA

Der Browser Opera verwendet nicht den Zertifikatsspeicher von Microsoft Windows. Bei der Verwendung von Opera ist es zur Untersuchung von SSL-Verbindungen erforderlich, das Kaspersky-Lab-Zertifikat manuell zu installieren.

Gehen Sie folgendermaßen vor, um das Kaspersky-Lab-Zertifikat zu installieren:

1. Wählen Sie im Menü des Browsers den Punkt **Tools** → **Einstellungen**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Erweitert**.
3. Wählen Sie auf der linken Fensterseite die Registerkarte **Sicherheit** und klicken Sie auf **Zertifikate verwalten**.
4. Wählen Sie im folgenden Fenster die Registerkarte **Zertifizierungsstellen** und klicken Sie auf **Importieren**.

5. Wählen Sie im folgenden Fenster die Datei des Kaspersky-Lab-Zertifikats. Pfad der Datei des Kaspersky-Lab-Zertifikats: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

6. Klicken Sie im folgenden Fenster auf **Installieren**. Das Kaspersky-Lab-Zertifikat wird installiert. Um Informationen zum Zertifikat anzuzeigen und die Aktionen, bei denen das Zertifikat verwendet werden soll, auszuwählen, wählen Sie das Zertifikat in der Liste und klicken Sie auf **Anzeigen**.

Gehen Sie folgendermaßen vor, um das Kaspersky-Lab-Zertifikat für Opera Version 9.x zu installieren:

1. Wählen Sie im Menü des Browsers den Punkt **Tools** → **Einstellungen**.

2. Wählen Sie im folgenden Fenster den Abschnitt **Erweitert**.

3. Wählen Sie auf der linken Fensterseite die Registerkarte **Sicherheit** und klicken Sie auf **Zertifikate verwalten**.

4. Wählen Sie im folgenden Fenster die Registerkarte **Zertifizierungsstellen** und klicken Sie auf **Importieren**.

5. Wählen Sie im folgenden Fenster die Datei des Kaspersky-Lab-Zertifikats. Pfad der Datei des Kaspersky-Lab-Zertifikats: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

6. Klicken Sie im folgenden Fenster auf **Installieren**. Das Kaspersky-Lab-Zertifikat wird installiert.

Wenn Ihr Computer mit dem Betriebssystem Microsoft Windows Vista arbeitet, lautet der Pfad der Zertifikatsdatei von Kaspersky Lab: *%AllUsersProfile%\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

NETZWERKMONITOR

Der Netzwerkmonitor dient dazu, in Echtzeit Informationen über die Netzwerkaktivität anzuzeigen.

Gehen Sie folgendermaßen vor, um den Netzwerkmonitor zu starten:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.

   Das Fenster **Computersicherheit** wird geöffnet.

2. Wählen Sie auf der linken Fensterseite **Schutz-Center**.

3. Öffnen Sie mit dem Link **Netzwerkmonitor** das Fenster **Netzwerkmonitor**, das Informationen über die Netzwerkaktivität enthält.

PROXYSERVER-EINSTELLUNGEN

Wenn die Internetverbindung über einen Proxyserver erfolgt, ist es erforderlich, die entsprechenden Verbindungsparameter anzupassen. Kaspersky PURE verwendet diese Einstellungen bei der Arbeit bestimmter Schutzkomponenten und für das Update der Datenbanken und Programm-Module.

Wenn in Ihrem Netzwerk ein Proxyserver installiert ist, der einen nicht standardmäßigen Port benutzt, ist es erforderlich, diesen Port zur Liste der kontrollierten Ports hinzuzufügen (s. Abschnitt "Liste der zu kontrollierenden Ports erstellen" auf S. 160).

Gehen Sie folgendermaßen vor, um die Proxyserver-Parameter anzupassen:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie auf der linken Fensterseite im Abschnitt **Allgemeine Einstellungen** den Abschnitt **Proxyserver**.

4. Aktivieren Sie das Kontrollkästchen **Proxyserver verwenden** und ändern Sie die Verbindungseinstellungen für den Proxyserver.

LISTE DER ZU KONTROLLIERENDEN PORTS ERSTELLEN

Bei der Arbeit von Schutzkomponenten wie Mail-Anti-Virus, Anti-Spam (s. S. 119), Web-Anti-Virus (auf S. 111) und IM-Anti-Virus werden die Datenströme kontrolliert, die mit bestimmten Protokollen und über bestimmte offene TCP-Ports Ihres Computers übertragen werden. Mail-Anti-Virus analysiert beispielsweise die Informationen, die per SMTP übertragen werden, während Web-Anti-Virus die HTTP-, HTTPS- und FTP-Pakete analysiert.

Sie können die Kontrolle aller oder nur bestimmter Netzwerkports aktivieren. Bei der Kontrolle bestimmter Ports kann eine Liste der Programme angelegt werden, für die alle Ports kontrolliert werden sollen. Es wird empfohlen, in diese Liste Programme aufzunehmen, die Daten per FTP-Protokoll senden oder empfangen.

- *Gehen Sie folgendermaßen vor, um einen Port zur Liste der kontrollierten Ports hinzuzufügen:*

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie auf der linken Fensterseite unter **Schutz-Center** den Abschnitt **Netzwerk**.

4. Klicken Sie auf der rechten Fensterseite auf **Auswählen**.

   Das Fenster **Netzwerkports** wird geöffnet.

5. Öffnen Sie über den Link **Hinzufügen** unterhalb der Portliste im oberen Fensterbereich das Fenster **Netzwerkport** und geben Sie Nummer und Beschreibung des Ports ein.

- *Gehen Sie folgendermaßen vor, um einen Port aus der Liste der kontrollierten Ports auszuschließen:*

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie auf der linken Fensterseite unter **Schutz-Center** den Abschnitt **Netzwerk**.

4. Klicken Sie auf der rechten Fensterseite auf **Auswählen**.

   Das Fenster **Netzwerkports** wird geöffnet.

5. Deaktivieren Sie in der Portliste im oberen Fensterbereich das Kontrollkästchen neben der Beschreibung des Ports, der deaktiviert werden soll.

- *Gehen Sie folgendermaßen vor, um eine Liste der Programme anzulegen, für die alle Ports kontrolliert werden sollen:*

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie auf der linken Fensterseite unter **Schutz-Center** den Abschnitt **Netzwerk**.

4. Klicken Sie auf der rechten Fensterseite auf **Auswählen**.

   Das Fenster **Netzwerkports** wird geöffnet.

5. Aktivieren Sie das Kontrollkästchen **Alle Ports für die angegebenen Programme kontrollieren** und aktivieren Sie in der darunter angeordneten Programmliste die Kontrollkästchen neben den Programmen, für die alle Ports kontrolliert werden sollen.

6. Ist ein Programm nicht in der Liste enthalten, können Sie es wie folgt hinzufügen:

   a. Um die Methode für das Hinzufügen von Programmen in die Liste auszuwählen, öffnen Sie das Menü über den Link **Hinzufügen** unterhalb der Programmliste und wählen Sie einen der folgenden Menüpunkte aus:

      - Wählen Sie den Punkt **Durchsuchen** aus, um den Speicherort der ausführbaren Datei des Programms anzugeben. Nach Auswahl der ausführbaren Datei öffnet sich das Fenster **Programm**.

      - Wählen Sie den Punkt **Programme**, um eines der derzeit laufenden Programme auszuwählen. Nach Auswahl eines Programms öffnet sich das Fenster **Programm**.

7. Geben Sie im Fenster **Programm** eine Beschreibung für das gewählte Programm ein.

VERTRAUENSWÜRDIGE ZONE

Die *vertrauenswürdige Zone* ist eine benutzerdefinierte Liste von Objekten, die nicht von dem Programm kontrolliert werden. Mit anderen Worten ist dies eine Auswahl von Ausnahmen für den Schutz, den Kaspersky PURE bietet.

Die vertrauenswürdige Zone wird auf Basis einer Liste der vertrauenswürdigen Programme (s. Abschnitt "Liste mit vertrauenswürdigen Programmen erstellen" auf S. 162) und der Ausnahmeregeln (s. Abschnitt "Ausnahmeregeln erstellen" auf S. 162) eingerichtet, wobei die Besonderheiten der Objekte, mit denen Sie arbeiten, sowie der Programme, die auf Ihrem Computer installiert sind, zu berücksichtigen sind. Die Aufnahme von Objekten in die vertrauenswürdige Zone kann beispielsweise erforderlich sein, wenn Kaspersky PURE den Zugriff auf ein bestimmtes Objekt oder Programm blockiert, Sie aber sicher sind, dass dieses Objekt / Programm absolut unschädlich ist.

Wenn Sie beispielsweise die Objekte, die von dem standardmäßigen Windows-Editor verwendet werden, für ungefährlich und ihre Untersuchung für nicht erforderlich halten, Sie diesem Programm also vertrauen, dann fügen Sie den Editor zur Liste der vertrauenswürdigen Programme hinzu, um die Objekte, die von diesem Prozess benutzt werden, von der Untersuchung auszuschließen.

Außerdem können bestimmte Aktionen, die als gefährlich klassifiziert werden, im Rahmen der Funktionalität bestimmter Programme ungefährlich sein. So ist das Abfangen eines über die Tastatur eingegebenen Texts für Programme zum automatischen Umschalten der Tastaturbelegung (z.B. Punto Switcher) eine normale Aktion. Um die Besonderheit solcher Programme zu berücksichtigen und die Kontrolle ihrer Aktivität abzuschalten, empfehlen wir, sie in die Liste der vertrauenswürdigen Anwendungen aufzunehmen.

Wenn ein Programm der vertrauenswürdigen Liste hinzugefügt wird, werden die Datei- und Netzwerkaktivität dieses Programms (einschließlich verdächtiger Aktivität) sowie seine Zugriffe auf die Systemregistrierung nicht kontrolliert. Zugleich werden die ausführbare Datei und der Prozess eines vertrauenswürdigen Programms weiterhin auf Viren untersucht. Um ein Programm vollständig von der Untersuchung auszuschließen, müssen die Ausnahmeregeln verwendet werden.

Durch das Ausschließen vertrauenswürdiger Programme von der Untersuchung lassen sich Kompatibilitätsprobleme von Kaspersky PURE mit anderen Programmen vermeiden (beispielsweise Probleme einer doppelten Untersuchung des Netzwerkverkehrs eines anderen Computers durch Kaspersky PURE und durch ein anderes Antiviren-Programm). Außerdem lässt sich dadurch die Leistungsfähigkeit des Computers erhöhen, was speziell bei der Verwendung von Serverprogrammen wichtig ist.

Die Ausnahmeregeln der vertrauenswürdigen Zone gewährleisten ihrerseits die Möglichkeit, mit legalen Programmen zu arbeiten, die von Angreifern für die Schädigung des Computers oder der Daten des Benutzers verwendet werden können. Solche Programme haben zwar selbst keine schädlichen Funktionen, können aber von Schadprogrammen als Hilfskomponenten missbrauch werden. Zu dieser Kategorie gehören beispielsweise Programme zur Remote-Verwaltung, IRC-Clients, FTP-Server, unterschiedliche Hilfsprogramme zum Beenden von Prozessen und zum Verstecken ihrer Arbeit, Tastaturspione, Programme zur Kennwortermittlung, Programme zur automatischen Einwahl auf kostenpflichtige Webseiten u.a. Derartige Programme können aufgrund der Arbeit von Kaspersky PURE gesperrt werden. Um das Sperren zu verhindern, können für die verwendeten Programme Ausnahmeregeln erstellt werden.

Eine *Ausnahmeregel* ist eine Kombination von Bedingungen, bei deren Erfüllung ein Objekt nicht von Kaspersky PURE untersucht wird. In allen übrigen Fällen wird dieses Objekt von allen Schutzkomponenten mit den festgelegten Parametern untersucht.

Die Ausnahmeregeln der vertrauenswürdigen Zone können von mehreren Programmkomponenten (z.B. Datei-Anti-Virus (s. Abschnitt "Datei-Anti-Virus" auf S. 99), Mail-Anti-Virus (s. Abschnitt "Mail-Anti-Virus" auf S. 106), Web-Anti-Virus (s. Abschnitt "Web-Anti-Virus" auf S. 111)), sowie bei der Ausführung von Untersuchungsaufgaben verwendet werden.

IN DIESEM ABSCHNITT

Liste mit vertrauenswürdigen Programmen erstellen 162

Ausnahmeregeln erstellen..... 162

LISTE MIT VERTRAUENSWÜRDIGEN PROGRAMMEN ERSTELLEN

Kaspersky PURE untersucht standardmäßig alle Objekte, die von einem beliebigen Programmprozess geöffnet, gestartet oder gespeichert werden sollen, und kontrolliert die Aktivität aller Programme und den von ihnen erzeugten Netzwerkverkehr. Die Programme der vertrauenswürdigen Liste werden von Kaspersky PURE von der Untersuchung ausgeschlossen.

Gehen Sie folgendermaßen vor, um ein Programm zur Liste der vertrauenswürdigen Programme hinzuzufügen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** den Abschnitt **Bedrohungen und Ausnahmen**.
4. Klicken Sie auf der rechten Fensterseite im Block **Ausnahmen** auf **Einstellungen**.
5. Klicken Sie im folgenden Fenster auf der Registerkarte **Vertrauenswürdige Programme** auf den Link **Hinzufügen**, um das Menü zur Programmauswahl zu öffnen, und wählen Sie im Menü einen Punkt aus::
   - Wählen Sie den Punkt **Durchsuchen** aus, um den Speicherort der ausführbaren Datei des Programms anzugeben. Nach Auswahl einer ausführbaren Datei öffnet sich das Fenster **Ausnahmen für Programme**.
   - Wählen Sie den Punkt **Programme**, um eines der derzeit laufenden Programme auszuwählen. Nach Auswahl eines Programms öffnet sich das Fenster **Ausnahmen für Programme**.
6. Aktivieren Sie im folgenden Fenster **Ausnahmen für das Programm** die Kontrollkästchen für die Arten der Programmaktivität, die nicht untersucht werden sollen.

Mit Hilfe der entsprechenden Links im unteren Bereich der Liste können Sie die Untersuchungseinstellungen für ein Programm ändern oder es aus der Liste löschen. Um ein Programm aus der Liste auszuschließen, ohne sie zu entfernen, deaktivieren Sie das Kontrollkästchen neben dem Programm.

AUSNAHMEREGELN ERSTELLEN

Falls Sie in Ihrer Arbeit Programme benutzen, die von Kaspersky PURE als illegal eingestuft werden und von Angreifen zur Schädigung des Computers oder der Daten des Benutzers verwendet werden können, empfehlen wir Ihnen, für diese Ausnahmen einzurichten.

Gehen Sie folgendermaßen vor, um eine Ausnahmeregel zu erstellen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** den Abschnitt **Bedrohungen und Ausnahmen**.

4. Klicken Sie auf der rechten Fensterseite im Block **Ausnahmen** auf **Einstellungen**.
5. Klicken Sie im folgenden Fenster auf der Registerkarte **Regeln für Ausnahmen** auf den Link **Hinzufügen**.
6. Geben Sie im folgenden Fenster **Ausnahmeregel** die Parameter der Ausnahmeregel an.

SICHERE UMGEBUNG FÜR DIE AUSFÜHRUNG VON PROGRAMMEN

Die Virtualisierung stellt eine sichere, vom eigentlichen Betriebssystem isolierte Umgebung dar. Sie dient zum Start von Programmen, an deren Sicherheit Zweifel bestehen.

Bei der Arbeit in der Sicheren Umgebung werden Objekte, die tatsächlich zum Betriebssystem gehören, nicht verändert. Selbst wenn Sie in der Sicheren Umgebung ein infiziertes Programm starten, bleiben seine Aktionen auf die virtuelle Umgebung beschränkt und haben keinen Einfluss auf das Betriebssystem.

Der Start von Internetbrowsern in der Sicheren Umgebung gewährleistet die gefahrlose Ansicht von Webressourcen und schützt den Computer dabei vor dem Eindringen schädlicher Programme und die Benutzerdaten vor unerlaubten Veränderungen oder dem Löschen. Andrerseits bietet er die Möglichkeit, alle Objekte zu löschen, die während einer Internetsitzung gesammelt wurden (temporäre Dateien, Cookies, Chronik der besuchten Webseiten usw.). Microsoft Internet Explorer gehört zur Liste der Programme, die standardmäßig in der Sicheren Umgebung gestartet werden.

Der Start eines Programms (s. Abschnitt "Start eines Programms in der Sicheren Umgebung" auf S. 164) in der Sicheren Umgebung erfolgt in Übereinstimmung mit dem ausgewählten Modus.. Zum schnellen Start von Programmen in der Sicheren Umgebung besteht die Möglichkeit, Verknüpfungen zu erstellen.

Damit Dateien, die in der Sicheren Umgebung gespeichert oder verändert werden, auch bei der Arbeit im normalen Modus verfügbar sind, muss der speziell dafür vorgesehene gemeinsame Ordner der Sicheren Umgebung verwendet werden. Dieser steht in der Sicheren Umgebung und im normalen Modus zur Verfügung. Dateien, die sich in diesem Ordner befinden, werden nicht bei einer Bereinigung der Sicheren Umgebung nicht gelöscht.

Auf Computern mit dem Betriebssystem Microsoft Windows XP x64 steht die Sichere Umgebung nicht zur Verfügung.

Auf Computern, die von Microsoft Windows XP x64 und Microsoft Windows 7 x64 verwaltet werden, kann die Funktionalität bestimmter Programme bei der Arbeit in der Sicheren Umgebung eingeschränkt sein. Beim Start solcher Programme erscheint eine entsprechende Meldung auf dem Bildschirm, wenn die Meldungen (s. S. 244) über das Ereignis **Die Funktionalität des Programms in der Sicheren Umgebung ist eingeschränkt** aktiviert wurden.

IN DIESEM ABSCHNITT

Start eines Programms in der Sicheren Umgebung 164

Liste der Programme erstellen, die in der Sicheren Umgebung gestartet werden sollen. 165

Verknüpfung für den Start von Programmen erstellen 166

Daten der Sicheren Umgebung bereinigen 166

Gemeinsamen Ordner verwenden 167

START EINES PROGRAMMS IN DER SICHEREN UMGEBUNG

Wenn für ein Programm nicht der Modus **Immer in der Sicheren Umgebung starten** festgelegt wurde, bestehen folgende Möglichkeiten, um das Programm in der Sicheren Umgebung zu starten:

- aus dem Kontextmenü von Microsoft Windows
- aus dem **Hauptfenster von Kaspersky PURE** (s. S. 47).
- mit Hilfe einer zuvor erstellten Verknüpfung (s. Abschnitt "Verknüpfung für den Start von Programmen erstellen" auf S. 166).

Wenn für ein Programm der Modus **Immer in der Sicheren Umgebung starten** festgelegt wurde, wird das Programm unabhängig von der Startmethode immer in der Sicheren Umgebung gestartet.

Für Programme, die in der Sicheren Umgebung gestartet wurden, besitzt das Programmfenster einen grünen Rahmen. Außerdem besitzen die Programme grüne Farbe in der Liste der Programme, die von Programmkontrolle kontrolliert werden (s. Abschnitt "Programmkontrolle" auf S. 138).

Es wird empfohlen, die Programme, mit denen Sie später in der Sicheren Umgebung arbeiten möchten, in der normalen Umgebung von Microsoft Windows zu installieren.

- *Gehen Sie folgendermaßen vor, um ein Programm in der Sicheren Umgebung aus dem Kontextmenü von Microsoft Windows zu starten:*

  1. Öffnen Sie durch Rechtsklick das Kontextmenü für das ausgewählte Objekt: Verknüpfung oder ausführbare Programmdatei.
  2. Wählen Sie im Kontextmenü den Punkt **In Sicherer Umgebung starten**.

- *Gehen Sie folgendermaßen vor, um ein Programm in der Sicheren Umgebung aus dem Hauptfenster von Kaspersky PURE zu starten:*

  1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.
  2. Gehen Sie im folgenden Fenster zum Abschnitt **Programmkontrolle**.
  3. Öffnen Sie im unteren Fensterbereich im Feld **Programme, die in der Sicheren Umgebung gestartet werden** das Kontextmenü für das entsprechende Programm und wählen Sie den Punkt **Starten**.

- *Gehen Sie folgendermaßen vor, um ein Programm mit Hilfe einer Verknüpfung zu starten:*

  1. Öffnen Sie den Ordner, in dem Sie die Verknüpfung erstellt haben.
  2. Starten Sie das Programm durch Doppelklick auf die Verknüpfung.

LISTE DER PROGRAMME ERSTELLEN, DIE IN DER SICHEREN UMGEBUNG GESTARTET WERDEN SOLLEN.

Im Fenster **Computersicherheit** (s. S. 49) kann eine Liste der Programme angelegt werden, die in der Sicheren Umgebung gestartet werden sollen. Diese Liste befindet sich im Abschnitt **Programmkontrolle**.

Wenn Sie ein Programm zur Liste hinzufügen, das es erlaubt, gleichzeitig mit mehreren Kopien von sich selbst zu arbeiten (beispielsweise, Windows Internet Explorer), dann läuft jede neue Kopie des Programms nach dem Hinzufügen zur Liste in Sicherer Umgebung. Beim Hinzufügen zur Liste eines Programms, das die Verwendung nur einer Kopie erlaubt, muss das Programm nach dem Hinzufügen neu gestartet werden.

Wenn ein Programm zur Liste der Programme, die in der Sicheren Umgebung gestartet werden sollen, hinzugefügt wird, kann der Modus **Immer in der Sicheren Umgebung starten** dafür festgelegt werden. Das bedeutet, dass das Programm unabhängig von der Startmethode (mit Hilfe der Standardmittel von Microsoft Windows oder mit Mitteln von Kaspersky PURE in der Sicheren Umgebung gestartet wird.

Es wird davon abgeraten, den Modus **Immer in der Sicheren Umgebung starten** für Systemprogramme und -Utilities zu verwenden, weil dadurch die Funktionsfähigkeit des Betriebssystems gestört werden kann.

- *Gehen Sie folgendermaßen vor, ein Programm zur Liste der Programme hinzuzufügen, die in der Sicheren Umgebung gestartet werden:*

  1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.
  2. Gehen Sie im folgenden Fenster zum Abschnitt **Programmkontrolle**.

3. Klicken Sie im unteren Fensterbereich im Feld **Programme, die in der Sicheren Umgebung gestartet werden** auf den Link **Hinzufügen**, um das Menü zu öffnen.

4. Wählen Sie im Kontextmenü das erforderliche Programm. Bei Auswahl des Punkts **Durchsuchen** wird ein Fenster geöffnet, in dem der Pfad der ausführbaren Datei angegeben werden muss. Bei Auswahl des Punkts **Programme** wird eine Liste der momentan aktiven Programme geöffnet. Anschließend wird das Programmsymbol zur Liste hinzugefügt.

   Um ein Programm aus der Liste für die Sichere Umgebung zu entfernen, markieren Sie es in der Liste und verwenden Sie den Link **Löschen**.

Gehen Sie folgendermaßen vor, damit ein Programm unabhängig von der Startmethode immer in der Sicheren Umgebung gestartet wird:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.

2. Gehen Sie im folgenden Fenster zum Abschnitt **Programmkontrolle**.

3. Öffnen Sie im unteren Fensterbereich im Feld **Programme, die in der Sicheren Umgebung gestartet werden** das Kontextmenü für das entsprechende Programm und wählen Sie den Punkt **Immer in Sicherer Umgebung starten**.

   Neben dem Menüpunkt wird nun ein Häkchen ✓ angezeigt.

VERKNÜPFUNG FÜR DEN START VON PROGRAMMEN ERSTELLEN

Zum schnellen Start von Programmen in der Sicheren Umgebung besteht in Kaspersky PURE die Möglichkeit, Verknüpfungen zu erstellen. So kann das erforderliche Programm gestartet werden, ohne das Programmhauptfenster oder das Kontextmenü von Microsoft Windows zu öffnen.

Gehen Sie folgendermaßen vor, um eine Verknüpfung für den Start eines Programms in der Sicheren Umgebung zu erstellen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.

2. Gehen Sie im folgenden Fenster zum Abschnitt **Programmkontrolle**.

3. Öffnen Sie im unteren Fensterbereich im Feld **Programme, die in der Sicheren Umgebung gestartet werden** das Kontextmenü für das entsprechende Programm und wählen Sie den Punkt **Verknüpfung erstellen**.

4. Geben Sie im folgenden Fenster an, wo und unter welchem Namen die Verknüpfung gespeichert werden soll. Standardmäßig wird die Verknüpfung im Ordner *Arbeitsplatz* des aktiven Computerbenutzers erstellt und erhält einen Namen, der dem Programmprozess entspricht.

DATEN DER SICHEREN UMGEBUNG BEREINIGEN

Beim Start eines Programms in der Sicheren Umgebung erfolgen alle Veränderungen, die durch die Arbeit eines Programms verursacht werden, nur innerhalb der virtuellen Umgebung. In der Grundeinstellung sind beim nächsten Start eines Programms alle während einer Sitzung in der Sicheren Umgebung vorgenommenen Änderungen und gespeicherten Dateien wieder verfügbar.

Wenn die Daten, die in der Sicheren Umgebung gespeichert sind, nicht mehr benötigt werden oder wenn für alle laufenden Programme die aktuellen Einstellungen in der gewöhnlichen Umgebung von Microsoft Windows wiederhergestellt werden sollen, können Sie die Bereinigung der Sicheren Umgebung verwenden.

Wenn Sie nicht möchten, dass für ein bestimmtes Programm beim nächsten Start die in der Sicheren Umgebung vorgenommenen Änderungen verfügbar sind, können Sie den Modus **Daten der Sicheren Umgebung beim Beenden löschen** dafür festlegen. Das bedeutet, dass Änderungen, die während der Programmsitzung vorgenommen werden, beim Beenden des Programms automatisch gelöscht werden.

Bevor Sie die Daten der Sicheren Umgebung bereinigen, sollten Sie sich vergewissern, dass alle Informationen, die künftig noch benötigt werden, im gemeinsamen Ordner gespeichert wurden. Andernfalls werden die Daten gelöscht und können nicht wiederhergestellt werden.

- *Gehen Sie folgendermaßen vor, um die Daten der Sicheren Umgebung zu bereinigen:*

  1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.
  2. Gehen Sie im folgenden Fenster zum Abschnitt **Programmkontrolle**.
  3. Verwenden Sie im unteren Fensterbereich im Feld **Programme, die in der Sicheren Umgebung gestartet werden** den Link **Leeren**.
  4. Bestätigen Sie die Datenbereinigung im folgenden Fenster.

- *Gehen Sie folgendermaßen vor, damit die Daten der Sicheren Umgebung jedes Mal gelöscht werden, wenn ein Programm beendet wird:*

  1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.
  2. Gehen Sie im folgenden Fenster zum Abschnitt **Programmkontrolle**.
  3. Öffnen Sie im unteren Fensterbereich im Feld **Programme, die in der Sicheren Umgebung gestartet werden** das Kontextmenü für das entsprechende Programm und wählen Sie den Punkt **Daten der Sicheren Umgebung beim Beenden löschen**.

     Neben dem Menüpunkt wird nun ein Häkchen angezeigt und das Programmsymbol in der Liste der Programme, die in der Sicheren Umgebung gestartet werden, erhält das Symbol .

     Damit Daten der Sicheren Umgebung nicht mehr gelöscht werden, wenn ein Programm beendet wird, klicken Sie erneut auf diesen Menüpunkt.

GEMEINSAMEN ORDNER VERWENDEN

Bei der Arbeit in der Sicheren Umgebung erfolgen alle Veränderungen, die durch die Arbeit eines Programms verursacht werden, nur innerhalb der virtuellen Umgebung und wirken sich nicht auf die normale Umgebung aus. Dateien, die in der Sicheren Umgebung gespeichert werden, gelangen auf diese Weise nicht in die normale Umgebung.

Damit die Dateien, mit denen ein Benutzer in der Sicheren Umgebung gearbeitet hat, auch in der normalen Umgebung zur Verfügung stehen, ist in Kaspersky PURE die Möglichkeit zur Verwendung eines *Gemeinsamen Ordners der Sicheren Umgebung* vorgesehen. Alle Dateien, die bei der Arbeit in der Sicheren Umgebung in diesem Ordner gespeichert werden, stehen in der normalen Umgebung zur Verfügung.

Der gemeinsame Ordner ist ein Ordner auf der Festplatte, der bei der Installation von Kaspersky PURE angelegt wird.

Der gemeinsame Ordner wird bei der Programminstallation im Ordner *%AllUsersProfile%\Application Data\Kaspersky Lab\SandboxShared* erstellt und sein Ort kann nicht verändert werden.

Im Explorer von Microsoft Windows besitzt der gemeinsame Ordner das Symbol . Auf den Ordner kann auch aus dem Hauptfenster von Kaspersky PURE zugegriffen werden.

- *Gehen Sie folgendermaßen vor, um den gemeinsamen Ordner aus dem Hauptfenster von Kaspersky PURE zu öffnen:*

  1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.
  2. Gehen Sie im folgenden Fenster zum Abschnitt **Programmkontrolle**.

3. Klicken Sie auf den Link **Gemeinsamer Ordner**. Dadurch wird der Ordner in einem Standardfenster des Explorers von Microsoft Windows geöffnet.

QUARANTÄNE UND BACKUP

Die *Quarantäne* ist ein spezieller Speicher, in den Objekte verschoben werden, die möglicherweise von Viren infiziert sind. *Möglicherweise infizierte Objekte* sind Objekte, die verdächtig sind, von Viren oder Virenmodifikationen infiziert zu sein.

Ein verdächtiges Objekt kann während der Virensuche sowie bei der Arbeit von Datei-Anti-Virus, Mail-Anti-Virus und Proaktiver Schutz gefunden und in die Quarantäne verschoben werden.

Objekte werden in folgenden Fällen in die Quarantäne verschoben:

- Der Objektcode besitzt Ähnlichkeit mit einer bekannten Bedrohung, wurde aber teilweise verändert, oder er erinnert an die Struktur eines Schadprogramms, ist aber nicht in den Datenbanken enthalten. In diesem Fall werden Objekte aufgrund einer heuristischen Analyse, die von Datei-Anti-Virus oder Mail-Anti-Virus ausgeführt wird oder bei einer Virensuche erfolgt, in die Quarantäne verschoben. Der heuristische Analysemechanismus führt nur selten zu einem Fehlalarm.

- Die Aktionsfolge, die von einem Objekt ausgeführt werden soll, gilt als verdächtig. In diesem Fall werden Objekte aufgrund einer Verhaltensanalyse, die vom Proaktiven Schutz ausgeführt wird, in die Quarantäne verschoben.

Ein Objekt unter Quarantäne zu stellen, bedeutet, es wird nicht kopiert, sondern verschoben: Das Objekt wird am ursprünglichen Speicherort oder aus einer E-Mail-Nachricht gelöscht und im Quarantäneordner gespeichert. Die unter Quarantäne stehenden Dateien werden in einem speziellen Format gespeichert und stellen keine Gefahr dar.

Das *Backup* dient zur Speicherung der Sicherungskopien für infizierte Objekte, die zum Zeitpunkt ihrer Entdeckung nicht desinfiziert werden können.

Möglicherweise kann die Bedrohung von Kaspersky PURE eindeutig bestimmt und desinfiziert werden, nachdem die Programm-Datenbanken aktualisiert wurden. Deshalb untersucht das Programm die Quarantäneobjekte nach jedem Update (s. S. 98).

IN DIESEM ABSCHNITT

Quarantäne- und Backup-Objekte speichern 168

Arbeit mit Objekten in der Quarantäne 169

QUARANTÄNE- UND BACKUP-OBJEKTE SPEICHERN

Die maximale Speicherdauer für Objekte beträgt standardmäßig 30 Tage. Danach werden die Objekte gelöscht. Sie können diese Zeitbeschränkung aufheben oder die maximale Speicherdauer für Objekte ändern.

Außerdem können Sie eine maximale Größe für die Quarantäne und das Backup festlegen. Beim Erreichen der maximalen Größe wird der Inhalt der Quarantäne und des Backups durch neue Objekte ersetzt. Die Größenbeschränkung ist standardmäßig deaktiviert.

Gehen Sie folgendermaßen vor, um eine maximale Speicherdauer für Objekte festzulegen:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie auf der linken Fensterseite im Abschnitt **Allgemeine Einstellungen** den Abschnitt **Berichte und Speicher**.

4. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Objekte speichern für maximal** und legen Sie eine maximale Speicherdauer für Quarantäneobjekte fest.

Gehen Sie folgendermaßen vor, um diee maximale Größe für die Quarantäne und das Backup anzupassen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Allgemeine Einstellungen** den Abschnitt **Berichte und Speicher**.
4. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Maximale Größe** und legen Sie eine maximale Größe für die Quarantäne und das Backup fest.

ARBEIT MIT OBJEKTEN IN DER QUARANTÄNE

Die Quarantäne von Kaspersky PURE ermöglicht die Ausführung folgender Operationen:

- Dateien, die Sie für infiziert halten, in die Quarantäne verschieben.
- Untersuchung und Desinfektion aller potentiell infizierten Objekte der Quarantäne unter Nutzung der aktuellen Datenbankversion von Kaspersky PURE.
- Wiederherstellung von Dateien in einem vom Benutzer gewählten Ordner oder (standardmäßig) in den Ordnern, aus denen sie in die Quarantäne verschoben wurden.
- Ein beliebiges Quarantäneobjekt oder eine Gruppe der Objekte löschen.
- Quarantäneobjekte zur Untersuchung an Kaspersky Lab schicken.

Ein Objekt kann auf zwei Arten in die Quarantäne verschoben werden:

- mit dem Link **In die Quarantäne verschieben** im Fenster **Schutzstatus**.
- mit Hilfe des Kontextmenüs für ein Objekt

Gehen Sie folgendermaßen vor, um vom Fenster Schutzstatus aus ein Objekt in die Quarantäne zu verschieben:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.
2. Klicken Sie im folgenden Fenster oben auf den Link **Quarantäne**, um das Fenster **Schutzstatus** zu öffnen.
3. Klicken Sie auf der Registerkarte **Erkannte Bedrohungen** auf den Link **In die Quarantäne verschieben**.
4. Wählen Sie im folgenden Fenster das Objekt, das in die Quarantäne verschoben werden soll.

Gehen Sie folgendermaßen vor, um ein Objekt mit Hilfe des Kontextmenüs in die Quarantäne zu verschieben:

1. Öffnen Sie das Fenster von Microsoft Windows Explorer und gehen Sie in den Ordner mit dem Objekt, das in die Quarantäne verschoben werden soll.
2. Öffnen Sie durch Rechtsklick das Kontextmenü für das Objekt und wählen Sie den Punkt **In die Quarantäne verschieben**.

Gehen Sie folgendermaßen vor, um ein Objekt in der Quarantäne zu untersuchen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auuf **Computersicherheit**.
2. Klicken Sie im folgenden Fenster oben auf den Link **Quarantäne**, um das Fenster **Schutzstatus** zu öffnen.

3. Wählen Sie auf der Registerkarte **Erkannte Bedrohungen** ein Untersuchungsobjekt aus
4. Öffnen Sie durch Rechtsklick das Kontextmenü für das Objekt und wählen Sie dort den Punkt **Untersuchen**.

Gehen Sie folgendermaßen vor, um eine Desinfektion aller Objekte in der Quarantäne durchzuführen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.
2. Klicken Sie im folgenden Fenster oben auf den Link **Quarantäne**, um das Fenster **Schutzstatus** zu öffnen.
3. Klicken Sie auf der Registerkarte **Erkannte Bedrohungen** auf den Link **Alle desinfizieren**.

Gehen Sie folgendermaßen vor, um eine Datei aus der Quarantäne wiederherzustellen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.
2. Klicken Sie im folgenden Fenster oben auf den Link **Quarantäne**, um das Fenster **Schutzstatus** zu öffnen.
3. Wählen Sie auf der Registerkarte **Erkannte Bedrohungen** ein Objekt aus, das wiederhergestellt werden soll.
4. Öffnen Sie durch Rechtsklick das Kontextmenü für das Objekt und wählen Sie dort den Punkt **Wiederherstellen**.

Gehen Sie folgendermaßen vor, um Objekte aus der Quarantäne zu entfernen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.
2. Klicken Sie im folgenden Fenster oben auf den Link **Quarantäne**, um das Fenster **Schutzstatus** zu öffnen.
3. Wählen Sie auf der Registerkarte **Erkannte Bedrohungen** ein Objekt aus, das gelöscht werden soll.
4. Öffnen Sie durch Rechtsklick das Kontextmenü für das Objekt und wählen Sie dort den Punkt **Aus der Liste löschen**.

Um ein Quarantäneobjekt zur Untersuchung anKaspersky Lab zu schicken, gehen Sie wie folgt vor.

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.
2. Klicken Sie im folgenden Fenster oben auf den Link **Quarantäne**, um das Fenster **Schutzstatus** zu öffnen.
3. Wählen Sie auf der Registerkarte **Erkannte Bedrohungen** das Objekt aus, das zur Untersuchung geschickt werden soll.
4. Öffnen Sie durch Rechtsklick das Kontextmenü für das Objekt und wählen Sie dort den Punkt **Senden**.

BACKUP

Beim Backup werden in einem speziellen Speicher Sicherungskopien für ausgewählte Dateien angelegt.

Als *Backup-Speicher* wird ein speziell dafür vorgesehener Bereich eines Laufwerks oder Datenträgers bezeichnet. Die Speicher werden von Backup-Aufgaben verwendet, um Sicherungskopien von Daten abzulegen.

Beim Anlegen eines Speichers (s. Abschnitt "Speicher anlegen" auf S. 171) wählt der Benutzer einen Datenträger, benennt den neuen Speicher und passt die Speicherung von Sicherungskopien an. Zusätzlich kann ein Kennwort für den Zugriff auf die Daten in diesem Speicher festgelegt werden. Anschließend werden Dienstinformationen über den Speicher auf dem Datenträger gespeichert.

Es werden Backup-Aufgaben erstellt, um Sicherungskopien von Daten anzulegen (s. Abschnitt "Backup-Aufgabe erstellen" auf S. 173). Als *Backup-Aufgabe* bezeichnet man eine benutzerdefinierte Auswahl von Parametern, die die zu kopierenden Daten, den Speicherort für die Sicherungskopien und die Kopierbedingungen festlegen. Aufgaben können wiederholt gestartet werden (manuell oder nach Zeitplan).

Die im Rahmen einer Aufgabe angelegten Sicherungskopien von Dateien werden in *Archiven* gespeichert. Backup-Archive werden in einem Speicher abgelegt und besitzen den gleichen Namen wie die Aufgabe.

Um Daten aus Sicherungskopien wiederherzustellen, wird die Wiederherstellungsprozedur (s. Abschnitt "Daten wiederherstellen" auf S. 174) gestartet oder das Wiederherstellungstool Kaspersky Restore Utility verwendet. Dateien können aus Sicherungskopien entweder am ursprünglichen Ort oder in einem bestimmten Ordner wiederhergestellt werden.

Alle Ereignisse, die mit dem Backup zusammenhängen, sind in einem Bericht enthalten (s. Abschnitt "Ereignisbericht anzeigen" auf S. 177).

IN DIESEM ABSCHNITT

Speicher anlegen 171

Bereits vorhandenen Speicher verbinden 172

Speicher leeren 172

Speicher löschen 173

Backup-Aufgabe erstellen 173

Backup starten 174

Daten wiederherstellen 174

Sicherungskopien suchen 175

Daten einer Sicherungskopie anzeigen 176

Ereignisbericht anzeigen 177

SPEICHER ANLEGEN

Es steht ein Assistent zur Verfügung, um Speicher anzulegen. Der Assistent für neue Speicher kann auf zwei Arten gestartet werden:

- aus dem Hauptfenster des Moduls.

- aus dem Assistenten für neue Backup-Aufgaben (s. Abschnitt "Backup-Aufgabe erstellen" auf S. 173)

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**, zum Abschluss des Assistenten die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf **Abbrechen** beendet werden.

Außerdem können Sie mit Hilfe der Links im oberen Fensterbereich zwischen den einzelnen Schritten des Assistenten navigieren.

Gehen Sie folgendermaßen vor, um einen Backup-Speicher anzulegen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Backup**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Backup-Speicher** und klicken Sie auf **Erstellen**.
3. Dadurch wird der Assistent für neue Backup-Speicher gestartet. Details zu den einzelnen Schritte des Assistenten:
   a. Wählen Sie auf der linken Seite des Fensters **Laufwerk** den Typ des Datenträgers, der als Speicher verwendet werden soll.

      Um die Daten besser zu schützen, wird empfohlen, die Backup-Speicher auf Wechseldatenträgern anzulegen.

   b. Legen Sie im Fenster **Schutz** ein Kennwort fest, um die Daten in diesem Speicher vor unerlaubtem Zugriff zu schützen (falls erforderlich).
   c. Beschränken Sie im Fenster **Dateiversionen** die Anzahl der Dateiversionen, die sich gleichzeitig im Speicher befinden dürfen, sowie die Speicherdauer für Dateiversionen (falls erforderlich).
   d. Geben Sie im Fenster **Übersicht** einen Namen für den neuen Speicher an und bestätigen Sie, dass der Speicher mit diesen Parametern erstellt werden soll.

BEREITS VORHANDENEN SPEICHER VERBINDEN

Wenn Sie mit Hilfe von Kaspersky PURE einen Speicher erstellt haben, dieser aber auf Ihrem Computer nicht verfügbar ist (z.B. nach einer Systemneuinstallation oder wenn der Speicher von einem anderen Computer kopiert wurde), ist es erforderlich, den Speicher zu verbinden, um mit den Daten arbeiten zu können.

Gehen Sie folgendermaßen vor, um einen vorhandenen Speicher zu verbinden:

1. Öffnen Sie das Programhauptfenster und klicken Sie auf **Backup**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Backup-Speicher** und klicken Sie auf **Verbinden**.
3. Wählen Sie einen Speichertyp und geben Sie im Fenster **Speicher verbinden** die Verbindungseinstellungen an.

   Wenn die Parameter korrekt angegeben wurden, erscheint der Speicher in der Liste.

SPEICHER LEEREN

Wenn ein Speicher zu wenig freien Platz aufweist, können Sie veraltete Versionen und Sicherungskopien von Dateien, die sich nicht auf dem Computer befinden, löschen.

Gehen Sie folgendermaßen vor, um die Berichte zu bereinigen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Backup**.

2. Wählen Sie im folgenden Fenster den Abschnitt **Backup-Speicher**.

3. Wählen Sie den Speicher, der geleert werden soll, und klicken Sie auf den Link **Leeren**.

4. Wählen Sie im folgenden Fenster **Speicher leeren** die Dateiversionen, die aus dem Speicher gelöscht werden sollen.

SPEICHER LÖSCHEN

Zum Löschen eines Backup-Speichers wird der Assistent zum Löschen eines Speichers verwendet. Beim Löschen werden die Aktionen für die Daten in dem zu löschenden Speicher und für die Aufgaben, die den Speicher zum Sicherungskopieren verwenden, festgelegt.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**, zum Abschluss des Assistenten die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf **Abbrechen** beendet werden.

Außerdem können Sie mit Hilfe der Schaltflächen im oberen Fensterbereich zwischen den einzelnen Schritten des Assistenten navigieren.

➧ *Gehen Sie folgendermaßen vor, um einen Backup-Speicher zu löschen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Backup**.

2. Wählen Sie im folgenden Fenster den Abschnitt **Backup-Speicher**.

3. Wählen Sie den Speicher, der geleert werden soll, und klicken Sie auf den Link **Löschen**.

4. Dadurch wird der Assistent zum Löschen eines Backup-Speichers gestartet. Details zu den einzelnen Schritte des Assistenten:

   a. Wählen Sie im Fenster **Inhalt** eine Aktion für die Sicherungskopien, die sich in dem zu löschenden Speicher befinden.

   b. Wählen Sie im Fenster **Aufgaben** eine Aktion für die Aufgaben, die den Speicher zum Sicherungskopieren verwenden.

   c. Bestätigen Sie im Fenster **Übersicht**, dass der Speicher gelöscht werden soll.

BACKUP-AUFGABE ERSTELLEN

Backup-Aufgaben dienen dazu, Sicherungskopien von Dateien anzulegen, und umfassen folgende Einstellungen:

- Auswahl der Dateien, für die Sicherungskopien angefertigt werden sollen.
- Speicher, in dem Sicherungskopien erstellt werden sollen.
- Bedingungen für den Start des Backup-Vorgangs.

Es steht ein Assistent zur Verfügung, um neue Aufgaben zu erstellen.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**, zum Abschluss des Assistenten die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf **Abbrechen** beendet werden.

Außerdem können Sie mit Hilfe der Schaltflächen im oberen Fensterbereich zwischen den einzelnen Schritten des Assistenten navigieren.

Gehen Sie folgendermaßen vor, um eine Backup-Aufgabe zu erstellen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Backup**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Backup** und klicken Sie auf **Erstellen**.
3. Dadurch wird der Assistent für neue Backup-Aufgaben gestartet. Details zu den einzelnen Schritte des Assistenten:
   a. Wählen Sie im Fenster **Inhalt** die Objekte, für die Sicherungskopien angefertigt werden sollen.
   b. Wählen Sie im Fenster **Speicher** den Speicher, in dem die Sicherungskopien abgelegt werden sollen.
   c. Legen Sie im Fenster **Zeitplan** die Startbedingungen für die Aufgabe fest.
   d. Geben Sie im Fenster **Übersicht** einen Namen für die neue Aufgabe an und bestätigen Sie, dass eine Aufgabe mit diesen Parametern erstellt werden soll.

BACKUP STARTEN

Backup-Aufgaben können automatisch (nach Zeitplan) oder manuell gestartet werden. Der momentan für den Aufgabenstart verwendete Modus wird in der Aufgabenliste genannt (s. Abbildung unten).

Dokumente von Eigene Dokumente
Wurde abgeschlossen vor 11 Minuten
Storage on drive C:\: frei 1,1 GB von 1,1 GB
Startmodus: Manuell

Abbildung 14. Backup-Aufgabe

Der Zeitplan für den automatischen Start wird beim Erstellen einer Aufgabe eingestellt und kann später geändert werden.

Bei Bedarf können jede Aufgabe manuell starten.

Gehen Sie folgendermaßen vor, um eine Backup-Aufgabe manuell zu starten:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Backup**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Backup**.
3. Wählen Sie auf der rechten Seite des Fensters in der Liste die Aufgabe, die ausgeführt werden soll, und klicken Sie auf **Ausführen**.

   In der Zeile der ausgewählten Aufgabe wird die Dauer seit dem Start der Ausführung angezeigt. Mit Hilfe der entsprechenden Schaltflächen kann die Aufgabenausführung angehalten oder abgebrochen werden.

   Durch die Ausführung einer Aufgabe wird im Speicher ein Archiv mit Sicherungskopien für das festgelegte Datum angelegt.

DATEN WIEDERHERSTELLEN

Falls erforderlich, können Daten aus den Sicherungskopien von Dateien wiederhergestellt werden. Der Wiederherstellungsvorgang ist nur für angeschlossene Speicher verfügbar. Bei der Wiederherstellung werden die Daten aus den Sicherungskopien im ausgewählten Ordner gespeichert.

Die Wiederherstellung von Dateien kann auf unterschiedliche Art erfolgen:

- letzte Version einer Datei wiederherstellen.

- wiederherzustellende Version nach Datum auswählen.

Gehen Sie folgendermaßen vor, um die letzte Version einer Datei wiederherzustellen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Backup**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Daten wiederherstellen**.
3. Wählen Sie den Speicher, in dem sich die erforderlichen Sicherungskopien befinden, und klicken Sie auf **Wiederherstellen**.
4. Wählen Sie im oberen Bereich des Fensters **Daten aus Speicher wiederherstellen** in der Dropdown-Liste **Archiv** den Namen der Aufgabe aus, bei deren Ausführung das Archiv mit den gesuchten Sicherungskopien erstellt wurde..
5. Wählen Sie die Dateien aus, die wiederhergestellt werden sollen. Aktivieren Sie dazu in der Liste die Kontrollkästchen der entsprechenden Dateien. Klicken Sie unter der Liste auf **Alle auswählen**, um alle Dateien auszuwählen. Klicken Sie im oberen Bereich des Fensters auf **Wiederherstellen**.
6. Geben Sie im folgenden Fenster **Wiederherstellung** an, wo wiederhergestellte Dateien gespeichert werden sollen, und legen Sie das Vorgehen bei einer Namensübereinstimmung fest. Klicken Sie auf **Wiederherstellen**.

Gehen Sie folgendermaßen vor, um die Version einer Datei auszuwählen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Backup**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Daten wiederherstellen**.
3. Wählen Sie den Speicher, in dem sich die erforderlichen Sicherungskopien befinden, und klicken Sie auf **Daten wiederherstellen**.
4. Wählen Sie im oberen Bereich des Fensters **Daten aus Speicher wiederherstellen** in der Dropdown-Liste **Archiv** den Namen der Aufgabe aus, bei deren Ausführung das Archiv mit den gesuchten Sicherungskopien erstellt wurde..
5. Wählen Sie die Datei aus, deren Version festgelegt werden soll. Aktivieren Sie dazu das Kontrollkästchen für die entsprechende Datei. Klicken Sie im oberen Fensterbereich auf **Versionen**.
6. Wählen Sie im folgenden Fenster **Dateiversionen** das Datum der wiederherzustellenden Version aus und klicken Sie auf **Wiederherstellen**.
7. Geben Sie im folgenden Fenster **Wiederherstellung** an, wo wiederhergestellte Dateien gespeichert werden sollen, und legen Sie das Vorgehen bei einer Namensübereinstimmung fest. Klicken Sie auf **Wiederherstellen**.

SICHERUNGSKOPIEN SUCHEN

Um in einem Speicher nach Sicherungskopien zu suchen, können Filter und Suchzeile der Liste verwendet werden.

Durch Verwendung eines Filters für Sicherungskopien werden nur jene Kopien angezeigt, die den festgelegten Suchkriterien entsprechen:

Mit der Suchzeile kann in einem Archiv über den Namen nach einer Sicherungskopie gesucht werden.

Damit die Sicherungskopien von Dateien angezeigt werden, die bei der letzten Aufgabenausführung nicht zur Liste der Backup-Dateien gehörten (die z.B. vom Computer gelöscht wurden), aktivieren Sie das Kontrollkästchen **Gelöschte Dateien anzeigen**.

Gehen Sie folgendermaßen vor, um Sicherungskopien zu filtern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Backup**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Daten wiederherstellen**.

3. Wählen Sie auf der rechten Fensterseite einen Speicher aus und klicken Sie auf **Wiederherstellen**.

4. Wählen Sie im oberen Bereich des Fensters **Daten wiederherstellen aus Speicher** die Suchkriterien für den Filter aus:

   - Wählen Sie aus der Dropdown-Liste **Archiv** den Namen der Aufgabe, bei deren Ausführung das Archiv mit den gesuchten Sicherungskopien erstellt wurde.

   - Wählen Sie in der Dropdown-Liste **Datum** das Datum aus, an dem das Archiv mit den benötigten Sicherungskopien erstellt wurde.

   - Wählen Sie aus der Dropdown-Liste **Kategorie** die Dateitypen, für die Sicherungskopien gesucht werden sollen.

Dadurch werden in der Liste nur jene Sicherungskopien angezeigt, die den ausgewählten Bedingungen entsprechen.

➧ *Gehen Sie folgendermaßen vor, um eine Sicherungskopie über ihren Namen zu suchen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Backup**.

2. Wählen Sie im folgenden Fenster den Abschnitt **Daten wiederherstellen**.

3. Wählen Sie auf der rechten Fensterseite einen Speicher aus und klicken Sie auf **Wiederherstellen**.

4. Geben im oberen Bereich des Fensters **Daten aus Speicher wiederherstellen** im Feld **Suche** den gesamten Dateinamen oder einen Teil davon ein.

Dadurch werden in der Liste nur jene Sicherungskopien angezeigt, deren Namen dem vorgegebenen Suchtext entspricht.

DATEN EINER SICHERUNGSKOPIE ANZEIGEN

Bevor Daten wiederhergestellt werden, kann der Inhalt der ausgewählten Sicherungskopie geprüft werden. Dazu kann man entweder die letzte Version öffnen oder eine Version für ein bestimmtes Datum auswählen.

➧ *Gehen Sie folgendermaßen vor, um die letzte Version einer Datei zu öffnen.*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Backup**.

2. Wählen Sie im folgenden Fenster den Abschnitt **Daten wiederherstellen**.

3. Wählen Sie den Speicher, in dem sich die erforderlichen Sicherungskopien befinden, und klicken Sie auf **Wiederherstellen**.

4. Wählen Sie im oberen Bereich des Fensters **Daten aus Speicher wiederherstellen** in der Dropdown-Liste **Archiv** den Namen der Aufgabe aus, bei deren Ausführung das Archiv mit den gesuchten Sicherungskopien erstellt wurde..

5. Wählen Sie auf der rechten Seite des Fensters die entsprechende Datei und klicken Sie auf **Öffnen**.

➧ *Gehen Sie folgendermaßen vor, um die Version einer Datei für ein bestimmtes Datum zu öffnen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Backup**.

2. Wählen Sie im folgenden Fenster den Abschnitt **Daten wiederherstellen**.

3. Wählen Sie den Speicher, in dem sich die erforderlichen Sicherungskopien befinden, und klicken Sie auf **Wiederherstellen**.

4. Wählen Sie im oberen Bereich des Fensters **Daten aus Speicher wiederherstellen** in der Dropdown-Liste **Archiv** den Namen der Aufgabe aus, bei deren Ausführung das Archiv mit den gesuchten Sicherungskopien erstellt wurde..

5. Wählen Sie auf der rechten Seite des Fensters die entsprechende Datei und klicken Sie auf **Versionen**.

6. Wählen Sie im folgenden Fenster **Dateiversionen** die erforderlichen Daten aus und klicken Sie auf **Öffnen**.

EREIGNISBERICHT ANZEIGEN

Alle Ereignisse, die mit dem Backup und der Datenwiederherstellung zusammenhängen, werden protokolliert.

Gehen Sie folgendermaßen vor, um einen Bericht über die Arbeit des Backup-Moduls zu erhalten:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Backup**.

2. Klicken Sie im oberen Bereich des folgenden Fensters auf den Link **Bericht**.

3. Passen Sie im folgenden Fenster **Bericht** die Darstellung der Ereignisinformationen an.

KINDERSICHERUNG

Die *Kindersicherung* bietet Kontrolle über die Aktionen unterschiedlicher Benutzer auf einem Computer und im Netzwerk. Die Kontrolle umfasst hierbei einerseits die Möglichkeit, den Zugriff auf Ressourcen und Programme zu beschränken, andrerseits die Anzeige von Berichten über die Benutzeraktionen.

Die Zahl der Kinder und Jugendlichen, die Zugang zu Computern und zum Internet besitzen, nimmt kontinuierlich zu. Dabei ergibt sich das Problem, die Sicherheit zu gewährleisten, weil Arbeit und Kommunikation im Internet mit einer ganzen Reihe von Risiken verbunden sind. Die wichtigsten Probleme sind:

- Webseiten, die Zeitverlust (Chats, Spielressourcen) oder Geldverlust (Internet-Shops, Auktionen) verursachen können.
- Zugriff auf Webressourcen, die für Erwachsene bestimmt sind (z.B. Seiten, die pornografische oder extremistische Materialien enthalten, die Themen wie Waffen, Drogen und Gewalt betreffen).
- Download von Dateien, die von Malware infiziert sind.
- unverhältnismäßig lange Arbeit am Computer und damit verbundene gesundheitliche Risiken.
- Kontakte mit Fremden, die sich als Gleichaltrige ausgeben und persönliche Informationen über den Benutzer erhalten können (z.B. echter Name, Adresse, Zeiten, zu denen Kinder unbeaufsichtigt zuhause sind).

Die Kindersicherung erlaubt es, die mit der Arbeit am Computer und im Internet verbundenen Risiken zu reduzieren. Dazu dienen folgende Funktionen des Programms:

- Zeitliche Beschränkung für die Verwendung des Computers und Internets.
- Erstellen von Listen für zum Start erlaubte und verbotene Programme, sowie vorübergehende Beschränkung des Starts von erlaubten Programmen.
- Erstellen von Listen mit Webseiten, auf die der Zugriff erlaubt bzw. verboten ist. Auswahl von inhaltlichen Kategorien für Webressourcen, die nicht zur Ansicht empfohlen sind.
- Aktivieren des Modus zur sicheren Suche mit Suchmaschinen (Links zu Webseiten mit verdächtigem Inhalt werden nicht in den Suchergebnissen angezeigt).
- Beschränkung des Downloads von Dateien aus dem Internet.
- Erstellen von Listen mit Kontakten, für die die Kommunikation über Instant Messenger und in sozialen Netzwerken erlaubt oder verboten wird.
- Kontrolle des Texts von Nachrichten, die mit Instant Messengern und in sozialen Netzwerken ausgetauscht werden.
- Verbot des Sendens von bestimmten persönlichen Daten.
- Suche nach bestimmten Schlüsselwörtern im Nachrichtentext.

Die Beschränkungen können einzeln aktiviert werden, wodurch sich die Kindersicherung flexibel auf unterschiedliche Benutzer anpassen lässt. Für jedes Benutzerkonto können Berichte angezeigt werden, die Ereignisse der kontrollierten Kategorien für einen bestimmten Zeitraum umfassen.

Um die Komponente zu verwalten, muss das Administratorkennwort eingegeben werden (s. Abschnitt "Wie der Zugriff auf die Einstellungen von Kaspersky PURE eingeschränkt wird" auf S. 77). Sollten Sie noch kein Kennwort für die Verwaltung von Kaspersky PURE festgelegt haben, so wird Ihnen vorgeschlagen, dies zu tun.

IN DIESEM ABSCHNITT

Kindersicherung für einen Benutzer anpassen 179

Berichte über die Aktionen eines Benutzers anzeigen 186

KINDERSICHERUNG FÜR EINEN BENUTZER ANPASSEN

Sie können die Kindersicherung für jedes Benutzerkonto individuell aktivieren und anpassen. Dazu werden für die einzelnen Benutzer entsprechende Beschränkungen festlegen, die z.B. vom Alter abhängig sind. Für Benutzer, deren Aktionen nicht kontrolliert werden sollen, können Sie die Kindersicherung deaktivieren.

Um die Komponente zu verwalten, ist eine Authentifizierung erforderlich. Nachdem der Administrator sein Kennwort eingegeben hat, kann er die Kindersicherung aktivieren, anhalten oder ausschalten sowie die Einstellungen ändern.

KONTROLLE AKTIVIEREN UND DEAKTIVIEREN

Sie können die Kindersicherung für jedes Benutzerkonto separat aktivieren und deaktivieren. Es ist beispielsweise überflüssig, die Aktionen eines erwachsenen Benutzers, der für den Computer über Administratorrechte verfügt, zu kontrollieren. Für ihn kann die Kindersicherung deaktiviert werden. Für die übrigen Benutzer, deren Aktionen kontrolliert werden soll, muss die Kindersicherung aktiviert und angepasst werden. Dazu können z.B. standardmäßige Einstellungen aus einer Vorlage geladen werden.

Die Kindersicherung kann für das aktuelle Benutzerkonto aus dem Hauptfenster oder aus dem Kontextmenü des Programmsymbols aktiviert und deaktiviert werden.

- *Gehen Sie folgendermaßen vor, um die Kindersicherung anzupassen:*

  1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Kindersicherung**.
  2. Wählen Sie im folgenden Fenster den Abschnitt **Benutzer** und klicken Sie oben auf **Aktivieren**.

- *Gehen Sie folgendermaßen vor, um die Kindersicherung anzuhalten:*

  1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Kindersicherung**.
  2. Wählen Sie im folgenden Fenster den Abschnitt **Benutzer** und klicken Sie oben auf **Anhalten**.
  3. Wählen Sie im Fenster **Kindersicherung anhalten**, in auf welche Art die Arbeit fortgesetzt werden soll.

Sie können die Kindersicherung für das aktuelle Benutzerkonto auch über das Hauptfenster von Kaspersky PURE (s. S. 47) oder aus dem Kontextmenü des Programmsymbols (s. S. 46) anhalten und fortsetzen.

SIEHE AUCH:

Einstellungen der Kindersicherung speichern und laden 179

EINSTELLUNGEN DER KINDERSICHERUNG SPEICHERN UND LADEN

Wenn Sie die Parameter der Kindersicherung bereits für ein Benutzerkonto angepasst haben, können diese in einer separaten Datei gespeichert werden. Zur schnellen Konfiguration können die Parameter aus dieser Datei später importiert werden. Außerdem können die Parameter, die für die Kontrolle eines anderen Benutzerkontos gelten,

übernommen oder es kann eine Konfigurationsvorlage verwendet werden (eine vordefinierte Auswahl von Regeln für unterschiedliche Benutzertypen, die sich an Alter, Erfahrung und anderen Merkmalen orientieren).

Nach einem Import können die festgelegten Parameter jederzeit für ein bestimmtes Benutzerkonto angepasst werden.

Gehen Sie folgendermaßen vor, um die Kontrollparameter in einer Datei zu speichern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Kindersicherung**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Benutzer**, gehen Sie dann auf das Benutzerkonto, für das Kontrollparameter gespeichert werden sollen, und klicken Sie auf **Anpassen**.
3. Verwenden Sie im oberen Bereich des folgenden Fensters den Link **Einstellungen exportieren** und speichern die Konfigurationsdatei.

Gehen Sie folgendermaßen vor, um Kontrollparameter aus einer Datei zu laden:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Kindersicherung**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Benutzer**, gehen Sie dann auf das Benutzerkonto, für das Kontrollparameter geladen werden sollen, und klicken Sie auf **Anpassen**.
3. Klicken Sie im oberen Bereich des folgenden Fensters auf den Link **Einstellungen laden**.
4. Wählen Sie im folgenden Fenster **Kontrolleinstellungen laden** die Variante **Datei mit zuvor gespeicherten Einstellungen** und geben Sie den Ort der Datei an.

Gehen Sie folgendermaßen vor, um die Parameter eines Benutzerkontos zu übernehmen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Kindersicherung**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Benutzer**, gehen Sie dann auf das Benutzerkonto, für das Kontrollparameter übernommen werden sollen, und klicken Sie auf **Anpassen**.
3. Klicken Sie im oberen Bereich des folgenden Fensters auf den Link **Einstellungen laden**.
4. Wählen Sie im folgenden Fenster **Kontrolleinstellungen laden** die Variante **Anderer Benutzer** und geben Sie das Benutzerkonto an, dessen Einstellungen verwendet werden sollen.

Gehen Sie folgendermaßen vor, um eine Konfigurationsvorlage zu verwenden:

1. Öffnen Sie das Programmhauptfenster und klicken Siie auf **Kindersicherung**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Benutzer**, gehen Sie dann auf das Benutzerkonto, für das Kontrollparameter übernommen werden sollen, und klicken Sie auf **Anpassen**.
3. Klicken Sie im oberen Bereich des folgenden Fensters auf den Link **Einstellungen laden**.
4. Wählen Sie im folgenden Fenster **Kontrolleinstellungen laden** die Variante **Vorlage** und geben Sie die Vorlage an, deren Einstellungen verwendet werden sollen.

DARSTELLUNG EINES BENUTZERKONTOS IN KASPERSKY PURE

Sie können ein Alias und ein Bild wählen, die in Kaspersky PURE für ein Benutzerkonto angezeigt werden sollen.

Gehen Sie folgendermaßen vor, um ein Alias und ein Bild für ein Benutzerkonto anzupassen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Kindersicherung**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Benutzer**, gehen Sie dann auf das Benutzerkonto, für das Kontrollparameter angepasst werden sollen, und klicken Sie auf **Anpassen**.

3. Wählen Sie im folgenden Fenster im Abschnitt **Erweitert** die Komponente **Darstellung**. Geben Sie ein Alias für das Benutzerkonto an und wählen Sie ein Bild.

ARBEITSZEIT AUF DEM COMPUTER

Sie können einen Zeitplan einrichten, der den Zugriff eines Benutzers auf den Computer reguliert (Wochentage und Zeiträume im Verlauf eines Tages). Außerdem kann die tägliche Gesamtdauer der Arbeit auf dem Computer begrenzt werden.

Kaspersky PURE warnt den Benutzer 15 und 5 Minuten vor Ablauf der für den Computer erlaubten Arbeitszeit davor, dass der Computer bald ausgeschaltet wird. Dadurch wird erlaubt, die Arbeit rechtzeitig abzuschließen und wichtige Daten zu speichern. Nach Ablauf der erlaubten Dauer meldet Kaspersky PURE einen Verstoß gegen den für die Computerverwendung festgelegten Zeitplan und fährt den Computer herunter.

Gehen Sie folgendermaßen vor, um die Verwendung des Computers zeitlich zu beschränken:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Kindersicherung**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Benutzer**, wählen Sie ein Benutzerkonto, für das eine Beschränkung festgelegt werden soll, und klicken Sie auf **Anpassen**.
3. Wählen Sie im folgenden Fenster im Abschnitt **Computer** die Komponente **Verwendung**.
4. Aktivieren Sie im folgenden Fenster **Arbeitszeit mit dem Computer kontrollieren** das Kontrollkästchen **Kontrolle aktivieren** und legen Sie die zeitlichen Beschränkungen fest.

START VON PROGRAMMEN

Sie können den Start bestimmter Programme erlauben oder verbieten. Außerdem kann der Start erlaubter Programme zeitlich eingeschränkt werden.

Gehen Sie folgendermaßen vor, um den Start von Programmen und Spielen zu beschränken:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Kindersicherung**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Benutzer**, wählen Sie ein Benutzerkonto, für das eine Beschränkung festgelegt werden soll, und klicken Sie auf **Anpassen**.
3. Wählen Sie im folgenden Fenster im Abschnitt **Computer** die Komponente **Start von Programmen**.
4. Aktivieren Sie im folgenden Fenster **Zu startende Programme kontrollieren** das Kontrollkästchen **Kontrolle aktivieren**.
5. Legen Sie auf den Registerkarten **Erlaubt** und **Verboten** die Listen mit Programmen an, deren Start erlaubt bzw. verboten ist. Passen Sie einen Zeitplan für die Verwendung von erlaubten Programmen an.

ARBEITSZEIT IM INTERNET

Sie können die Zeit, die ein Benutzer im Internet verbringen darf, beschränken. Passen Sie dazu einen Zeitplan für den Internetzugriff an (Wochentage und Zeiträume im Verlauf eines Tages, in denen der Zugriff erlaubt oder verboten ist). Außerdem kann die tägliche Gesamtdauer der Arbeit auf dem Computer begrenzt werden.

Kaspersky PURE warnt den Benutzer 10 Minuten vor Ablauf der für das Internet erlaubten Arbeitszeit davor, dass die Verbindung bald getrennt wird. Dadurch wird erlaubt, die Arbeit rechtzeitig abzuschließen und wichtige Daten zu speichern. Nach Ablauf der erlaubten Dauer meldet Kaspersky PURE einen Verstoß gegen den für die Internetverwendung festgelegten Zeitplan und trennt die Internetverbindung.

Gehen Sie folgendermaßen vor, um die Verwendung des Internets zu beschränken:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Kindersicherung**.

2. Wählen Sie im folgenden Fenster den Abschnitt **Benutzer**, wählen Sie ein Benutzerkonto, für das eine Beschränkung festgelegt werden soll, und klicken Sie auf **Anpassen**.

3. Wählen Sie im folgenden Fenster im Abschnitt **Internet** die Komponente **Verwendung**.

4. Aktivieren Sie im folgenden Fenster **Kontrolle für die Verwendung des Internets** das Kontrollkästchen **Kontrolle aktivieren** und legen Sie die zeitlichen Beschränkungen fest.

BESUCH VON WEBSEITEN

Sie können den Zugriff auf bestimmte Webressourcen in Abhängigkeit von ihrem Inhalt beschränken. Dazu können Listen mit erlaubten und verbotenen Webadressen angelegt werden. Außerdem können Kategorien von Webseiten ausgewählt werden, auf die der Zugriff blockiert werden soll.

Gehen Sie folgendermaßen vor, um den Zugriff auf Webressourcen zu beschränken:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Kindersicherung**.

2. Wählen Sie im folgenden Fenster den Abschnitt **Benutzer**, wählen Sie ein Benutzerkonto, für das eine Beschränkung festgelegt werden soll, und klicken Sie auf **Anpassen**.

3. Wählen Sie im folgenden Fenster im Abschnitt **Internet** die Komponente **Besuch von Webseiten**.

4. Aktivieren Sie im folgenden Fenster **Kontrolle für den Besuch von Webseite**n das Kontrollkästchen **Kontrolle aktivieren** und legen Sie Beschränkungen für den Besuch von Webseiten fest..

   Die Adressen von Webressourcen, auf die der Zugriff erlaubt und verboten ist, werden auf den Registerkarten **Verbotene Webadressen** und **Erlaubte Webadressen** angegeben. Auf der Registerkarte **Nicht empfohlen** können Kategorien von Webseiten ausgewählt werden, auf die der Zugriff blockiert werden soll.

5. Wenn Sie nur den Zugriff auf die aufgezählten erlaubten Webseiten zulassen möchten, aktivieren Sie das Kontrollkästchen **Besuch aller Webseiten verbieten, unter Ausnahme der Liste für erlaubte Webadressen**.

Wenn das Kontrollkästchen **Besuch aller Webseiten verbieten, unter Ausnahme der Liste für erlaubte Webadressen** aktiviert wurde, muss für eine Internetverbindung über einen Proxyserver die Adresse des Proxyservers zur Liste **Erlaubte Webadressen** hinzugefügt werden.

DOWNLOAD VON DATEIEN AUS DEM INTERNET

Sie können die Dateitypen, die aus dem Internet heruntergeladen werden dürfen, einschränken.

Gehen Sie folgendermaßen vor, um den Download von Dateien aus dem Internet zu beschränken:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Kindersicherung**.

2. Wählen Sie im folgenden Fenster den Abschnitt **Benutzer**, wählen Sie ein Benutzerkonto, für das eine Beschränkung festgelegt werden soll, und klicken Sie auf **Anpassen**.

3. Wählen Sie im folgenden Fenster im Abschnitt **Internet** die Komponente **Download von Dateien**.

4. Aktivieren Sie im folgenden Fenster **Kontrolle des Downloads von Dateien aus dem Internet** das Kontrollkästchen **Kontrolle aktivieren** und wählen Sie die Dateikategorien, für die der Download erlaubt ist..

MODUS FÜR SICHERE SUCHE

Einige Suchmaschinen versuchen, ihre Nutzer vor unzulässigen Inhalten auf Webseiten zu schützen. Dazu werden Webseiten bei der Indizierung auf Schlüsselwörter und Phrasen, Adressen und Ressourcenkategorien hin analysiert. Wenn der Modus für sichere Suche aktiviert ist, werden Seiten, die unerwünschten Kategorien angehören (Pornografie,

Drogen, Gewalt und sonstige Materialien, die nicht für Minderjährige geeignet sind), von den Suchergebnissen ausgeschlossen.

Die Kindersicherung erlaubt es, den sicheren Suchmodus gleichzeitig für die Suchmaschinen Google und Bing zu aktivieren.

Gehen Sie folgendermaßen vor, um den Modus für sichere Suche zu aktivieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Kindersicherung**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Benutzer**, wählen Sie ein Benutzerkonto, für das eine Beschränkung festgelegt werden soll, und klicken Sie auf **Anpassen**.
3. Wählen Sie im folgenden Fenster im Abschnitt **Internet** die Komponente **Sichere Suche**.
4. Aktivieren Sie im folgenden Fenster **Kontrolle der Suchergebnisse** das Kontrollkästchen **Kontrolle aktivieren**.

KORRESPONDENZ ÜBER INSTANT MESSENGER

Die Kontrolle der Korrespondenz mit Programmen zum Nachrichtensofortversand (Instant Messenger) umfasst die Kontrolle von erlaubten Kontakten sowie des Inhalts der Korrespondenz. Sie können Listen mit erlaubten und verbotenen Kontakten anlegen, Schlüsselwörter festlegen (s. Abschnitt "Schlüsselwörter suchen" auf S. 186), auf deren Vorhandensein die Nachrichten überprüft werden, und persönliche Daten (s. Abschnitt "Senden vertraulicher Informationen" auf S. 185), die nicht gesendet werden dürfen, angeben.

Wenn die Korrespondenz mit einem Kontakt verboten ist, werden alle Nachrichten, die sich an diesen Kontakt richten oder von ihm stammen, blockiert. Informationen über blockierte Nachrichten und das Vorhandensein von Schlüsselwörtern in Nachrichten werden protokolliert. Der vollständige Bericht enthält sogar die Nachrichtentexte für jeden Kontakt.

Die Kontrolle der Korrespondenz besitzt folgende Einschränkungen:

- Wenn ein Instant Messenger gestartet wurde, bevor die Kindersicherung aktiviert wurde, erfolgt die Korrespondenz-Kontrolle erst nach einem Neustart des Instant Messengers.
- Bei Verwendung eines HTTP-Proxies erfolgt keine Korrespondenz-Kontrolle.

Die aktuelle Version der Kindersicherung bietet die Kontrolle über folgende Instant Messenger:

- ICQ
- QIP
- Windows Live Messenger (MSN)
- Yahoo Messenger
- GoogleTalk
- mIRC
- Mail.Ru Agent
- Psi
- Miranda
- AOL Instant Messenger (AIM)
- Jabber

Viele Instant Messenger verwenden eine geschützte Verbindung. Um die Korrespondenz, die über solche Programme erfolgt, zu kontrollieren, muss die Untersuchung von geschützten Verbindungen157 aktiviert werden (s. S.).

- *Gehen Sie folgendermaßen vor, um die Kontakte, für die die Korrespondenz über Instant Messenger erlaubt ist, zu beschränken:*

  1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Kindersicherung**.
  2. Wählen Sie im folgenden Fenster den Abschnitt **Benutzer**, wählen Sie ein Benutzerkonto, für das eine Beschränkung festgelegt werden soll, und klicken Sie auf **Anpassen**.
  3. Wählen Sie im folgenden Fenster im Abschnitt **Kommunikation** die Komponente **Instant Messaging**.
  4. Aktivieren Sie im folgenden Fenster **Korrespondenz über Instant Messenger kontrollieren** das Kontrollkästchen **Kontrolle aktivieren**.
  5. Legen Sie auf den Registerkarten **Erlaubt** und **Verboten** die Listen mit erlaubten und verbotenen Kontakten an.
  6. Wählen Sie aus der Dropdown-Liste **Aktion** eine Standardaktion für die Kontakte, die nicht auf den Listen stehen.

  Sie können die Korrespondenz mit einem bestimmten Kontakt auch aus dem Detailbericht über Ereignisse für dieses Benutzerkonto erlauben oder verbieten.

- *Gehen Sie folgendermaßen vor, um eine Kurzstatistik anzuzeigen:*

  1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Kindersicherung**.
  2. Gehen Sie im folgenden Fenster zum Abschnitt **Berichte** und wählen Sie rechts in der Dropdown-Liste ein Benutzerkonto, für das ein Bericht angezeigt werden soll.

     Im Block **Kommunikation** wird für das ausgewählte Benutzerkonto eine Kurzstatistik für die Korrespondenz über Instant Messenger angezeigt.

- *Gehen Sie folgendermaßen vor, um einen ausführlichen Bericht anzuzeigen:*

  1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Kindersicherung**.
  2. Gehen Sie im folgenden Fenster zum Abschnitt **Berichte** und wählen Sie rechts in der Dropdown-Liste ein Benutzerkonto, für das ein Bericht angezeigt werden soll. Klicken Sie auf den Link **Detaillierter Bericht**.
  3. Wählen Sie im folgenden Fenster im Abschnitt **Kommunikation** die Komponente **Instant Messaging**.

     Im folgenden Fenster **Instant Messaging** wird ein ausführlicher Bericht angezeigt.

  Außerdem können Sie im Abschnitt **Benutzer** mit der Schaltfläche **Detaillierter Bericht** einen detaillierten Bericht öffnen.

KORRESPONDENZ IN SOZIALEN NETZWERKEN

Die Kontrolle der Korrespondenz über soziale Netzwerke umfasst die Kontrolle der erlaubten Kontakte und des Nachrichteninhalts. Sie können Listen mit erlaubten und verbotenen Kontakten anlegen, Schlüsselwörter festlegen (s. Abschnitt "Schlüsselwörter suchen" auf S. 186), auf deren Vorhandensein die Nachrichten überprüft werden, und persönliche Daten (s. Abschnitt "Senden vertraulicher Informationen" auf S. 185), die nicht gesendet werden dürfen, angeben.

Wenn die Korrespondenz mit einem Kontakt verboten ist, werden alle Nachrichten, die sich an diesen Kontakt richten oder von ihm stammen, blockiert. Informationen über blockierte Nachrichten und das Vorhandensein von Schlüsselwörtern in Nachrichten werden protokolliert. Der vollständige Bericht enthält sogar die Nachrichtentexte für jeden Kontakt.

Manche sozialen Netzwerke wie z.B. Twitter verwenden eine geschützte Verbindung. Um den Datenverkehr dieser Netzwerke zu untersuchen, muss die Untersuchung von geschützten Verbindungen aktiviert werden (s. S. 157).

Die aktuelle Version der Kindersicherung bietet die Kontrolle über folgende soziale Netzwerke:

- Facebook
- Twitter
- MySpace

Gehen Sie folgendermaßen vor, um die Kontakte, für die die Korrespondenz über soziale Netzwerke möglich ist, zu beschränken:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Kindersicherung**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Benutzer**, wählen Sie ein Benutzerkonto, für das eine Beschränkung festgelegt werden soll, und klicken Sie auf **Anpassen**.
3. Wählen Sie im folgenden Fenster im Abschnitt **Kommunikation** die Komponente **Soziale Netzwerke**.
4. Aktivieren Sie im folgenden Fenster **Korrespondenz in sozialen Netzwerken kontrollieren** das Kontrollkästchen **Kontrolle aktivieren**.
5. Wählen Sie aus der Dropdown-Liste **Aktion** eine Standardaktion für die Kontakte, die nicht auf den Listen stehen.

   Sie können die Korrespondenz mit einem bestimmten Kontakt auch aus dem Detailbericht über Ereignisse für dieses Benutzerkonto erlauben oder verbieten.

6. Schließen Sie das Konfigurationsfenster und klicken Sie auf **Detailbericht**.
7. Wählen Sie im folgenden Fenster im Abschnitt **Kommunikation** die Komponente **Soziale Netzwerke**.

   Im folgenden Fenster befindet sich rechts eine Liste der Kontakte, von denen eine Nachricht empfangen oder an die eine Nachricht gesendet wurde.

8. Geben Sie eine Aktion für die gewählten Kontakte an (Korrespondenz verbieten oder erlauben).

   Die Kontakte werden automatisch zur Liste der kontrollierten Kontakte hinzugefügt, die sich im Fenster **Einstellungen** im Abschnitt **Soziale Netzwerke** befindet.

SENDEN VERTRAULICHER INFORMATIONEN

Sie können verbieten, dass Daten, die persönliche Informationen enthalten, über Instant Messenger, soziale Netzwerke und beim Senden von Daten über Webseiten verschickt werden. Dafür ist es erforderlich, eine Liste mit Einträgen anzulegen, die vertrauliche Informationen enthalten (z.B. Adresse, Telefonnummer usw.).

Versuche zum Senden von Daten aus dieser Liste werden blockiert und es werden Informationen über blockierte Nachrichten im Bericht aufgezeichnet.

Gehen Sie folgendermaßen vor, um das Senden von persönlichen Daten zu blockieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Kindersicherung**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Benutzer**, wählen Sie ein Benutzerkonto, für das eine Beschränkung festgelegt werden soll, und klicken Sie auf **Anpassen**.
3. Wählen Sie im folgenden Fenster im Abschnitt **Kommunikation** die Komponente **Persönliche Daten**.

4. Aktivieren Sie im folgenden Fenster **Senden von persönlichen Daten kontrollieren** das Kontrollkästchen **Kontrolle aktivieren**. Fügen Sie der Liste für Daten, die nicht gesendet werden dürfen, mit dem Link **Hinzufügen** einen Eintrag hinzu.

SCHLÜSSELWÖRTER SUCHEN

Sie können kontrollieren, ob in der Korrespondenz eines Benutzers, die über Instant Messenger, soziale Netzwerke und beim Senden von Daten über Webseiten erfolgt, bestimmte Wörter oder Phrasen vorkommen.

Das Vorhandensein von festgelegten Schlüsselwörtern in ausgetauschten Nachrichten wird protokolliert.

Wenn die Korrespondenz-Kontrolle für Instant Messenger und soziale Netzwerke oder die Kontrolle für den Besuch von Webseiten deaktiviert ist, erfolgt keine Suche nach Schlüsselwörtern.

Gehen Sie folgendermaßen vor, um zu prüfen, ob bestimmte Wörter in der Korrespondenz vorhanden sind:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Kindersicherung**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Benutzer**, wählen Sie ein Benutzerkonto, für das eine Beschränkung festgelegt werden soll, und klicken Sie auf **Anpassen**.
3. Wählen Sie im folgenden Fenster im Abschnitt **Kommunikation** die Komponente **Schlüsselwörter**.
4. Aktivieren Sie im folgenden Fenster **Verwendung von Schlüsselwörtern kontrollieren** das Kontrollkästchen **Kontrolle aktivieren**. Fügen der Liste für Schlüsselwörter, die bei der Korrespondenz kontrolliert werden sollen, mit dem Link **Hinzufügen** einen Eintrag hinzu.

BERICHTE ÜBER DIE AKTIONEN EINES BENUTZERS ANZEIGEN

Sie können für jeden Benutzer, für den die Kindersicherung angepasst wurde, eine Kurzstatistik und einen ausführlichen Bericht für die Kategorien der kontrollierten Ereignisse anzeigen.

Gehen Sie folgendermaßen vor, um eine Kurzstatistik anzuzeigen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Kindersicherung**.
2. Gehen Sie im folgenden Fenster zum Abschnitt **Berichte** und wählen Sie rechts in der Dropdown-Liste ein Benutzerkonto, für das eine Kurzstatistik angezeigt werden soll.
3. In diesem Fenster wird für das ausgewählte Benutzerkonto eine Kurzstatistik angezeigt.

Gehen Sie folgendermaßen vor, um einen ausführlichen Bericht anzuzeigen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Kindersicherung**.
2. Gehen Sie im folgenden Fenster zum Abschnitt **Berichte** und wählen Sie rechts in der Dropdown-Liste ein Benutzerkonto, für das ein Bericht angezeigt werden soll. Klicken Sie auf den Link **Detaillierter Bericht**.
3. Im folgenden Fenster wird ein ausführlicher Bericht über die Kategorien für das ausgewählte Benutzerkonto angezeigt.

Außerdem können Sie im Abschnitt **Benutzer** mit der Schaltfläche **Detaillierter Bericht** einen detaillierten Bericht öffnen.

DATENVERSCHLÜSSELUNG

Die Datenverschlüsselung dient dazu, sensible Daten vor unerlaubtem Zugriff zu schützen. Dazu werden die Informationen in verschlüsselter Form in einem speziellen Container gespeichert.

Ein *Container* ist ein verschlüsseltes Objekt, das vom Benutzer mit Hilfe der Funktion zur Datenverschlüsselung angelegt wird. In einem Container werden Dateien und Ordner gespeichert. Für den Zugriff auf Daten, die sich in einem Container befinden, ist die Eingabe des Kennworts erforderlich. Außerdem muss das Programm Kaspersky PURE auf dem Computer installiert sein.

Um mit den Daten in einem Container zu arbeiten, müssen diese entschlüsselt werden. Dabei fragt Kaspersky PURE nach dem Zugriffskennwort. Nachdem das Kennwort erfolgreich eingegeben wurde, wird der Container im System als virtueller Wechseldatenträger angezeigt, auf den Dateien und Ordner mit Daten kopiert und gespeichert werden können.

IN DIESEM ABSCHNITT

Bereits vorhandenen Speicher erstellen und verbinden 187

Zugriff auf Daten in einem Container blockieren und freigeben 188

Dateien zu einem Container hinzufügen 189

Einstellungen eines Containers anpassen 189

Verknüpfung für den schnellen Zugriff auf einen Container erstellen 190

BEREITS VORHANDENEN SPEICHER ERSTELLEN UND VERBINDEN

Um Daten in verschlüsselter Form zu speichern, muss ein Container angelegt werden. Ein Container kann auf einem lokalen Datenträger oder auf einem Wechseldatenträger erstellt werden.

Es steht ein Assistent zur Verfügung, um neue Container zu erstellen. Beim Anlegen eines Containers werden Name, Größe, Kennwort und Ort der Containerdatei festgelegt.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**, zum Abschluss des Assistenten die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf **Abbrechen** beendet werden.

Außerdem können Sie mit Hilfe der Schaltflächen im oberen Fensterbereich zwischen den einzelnen Schritten des Assistenten navigieren.

Außerdem kann auch ein vorhandener Container verbunden werden, wenn er auf diesem Computer verfügbar ist (z.B. nach dem Neuaufsetzen des Systems oder wenn der Container von einem anderen Rechner kopiert wurde). In diesem Fall erscheint der Container auf der Liste, wobei der Zugriff auf ihn aber gesperrt ist. Um mit den Daten in einem Container zu arbeiten, müssen diese entschlüsselt (s. Abschnitt "Zugriff auf Daten in einem Container blockieren und freigeben" auf S. 188) werden.

Gehen Sie folgendermaßen vor, um einen Container anzulegen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Datenverschlüsselung**.
2. Klicken Sie im folgenden Fenster auf die die Schaltfläche **Container erstellen**.
3. Dadurch wird der Assistent für neue verschlüsselte Container gestartet. Details zu den einzelnen Schritte des Assistenten:
    a. Geben Sie im Fenster **Allgemeine Parameter** einen Namen, die Größe und ein Kennwort für den Container an.

b. Legen Sie im Fenster **Pfad** den Ort der Containerdatei fest.

c. Wählen Sie einen Buchstaben für das virtuelle Laufwerk, legen Sie bei Bedarf zusätzliche Einstellungen fest und bestätigen Sie im Fenster **Übersicht**, dass ein Container mit den genannten Einstellungen angelegt werden soll.

Gehen Sie folgendermaßen vor, um einen vorhandenen Container zu verbinden:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Datenverschlüsselung**.
2. Klicken Sie im folgenden Fenster auf die die Schaltfläche **Container verbinden**.
3. Geben Sie im folgenden Fenster einen Ort für die Containerdatei an.

ZUGRIFF AUF DATEN IN EINEM CONTAINER BLOCKIEREN UND FREIGEBEN

Nachdem ein Container erstellt wurde, ist der Zugriff auf die Daten freigegeben. Wenn ein vorhandener Container verbunden wurde, ist der Zugriff auf ihn standardmäßig gesperrt. Um mit den Daten in einem Container zu arbeiten, müssen diese entschlüsselt werden. Dazu kann das Interface von Kaspersky PURE oder das Kontextmenü von Microsoft Windows verwendet werden.

Wenn sich der Container auf einem Wechseldatenträger befindet, können Sie festlegen, dass beim Anschließen des Datenträgers der Zugriff auf die Daten im Container automatisch freigegeben wird.

Wenn der Zugriff auf einen Container freigegeben ist, steht der Container für alle Benutzerkonten des Computers in der Geräteliste als Wechseldatenträger zu Verfügung. Deshalb wird empfohlen, den Zugriff zu blockieren (die Daten im Container zu verschlüsseln), wenn Sie nicht mit den Daten arbeiten. Die Daten in einem Container können über das Programminterface von Kaspersky PURE oder über das Kontextmenü von Microsoft Windows verschlüsselt werden.

Gehen Sie folgendermaßen vor, um die Daten in einem Container über das Programminterface zu entschlüsseln:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Datenverschlüsselung**.
2. Klicken Sie im folgenden Fenster auf **Daten entschlüsseln**.
3. Passen Sie im folgenden Fenster die Datenentschlüsselung an und bestätigen Sie die Zugriffserlaubnis.

Gehen Sie folgendermaßen vor, um die Daten über das Kontextmenü zu entschlüsseln:

1. Öffnen Sie durch Rechtsklick das Kontextmenü der Containerdatei oder der Verknüpfung für den Zugriff auf den Container (s. Abschnitt "Verknüpfung für den Container erstellen" auf S. 190) auf dem Desktop.
2. Wählen Sie im folgenden Menü den Punkt **Daten entschlüsseln**.

Gehen Sie folgendermaßen vor, damit der Zugriff auf die Daten in einem Container beim Anschließen eines Datenträgers automatisch freigegeben wird:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Datenverschlüsselung**.
2. Wählen Sie im folgenden Fenster einen Container aus, auf den der Zugriff freigegeben ist, und klicken Sie auf **Anpassen**.
3. Aktivieren Sie im folgenden Fenster das Kontrollkästchen **Beim Anschließen entschlüsseln**.

Geben Sie folgendermaßen vor, um die Daten über die Programmoberfläche zu verschlüsseln:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Datenverschlüsselung**.
2. Wählen Sie im folgenden Fenster einen Container aus, auf den der Zugriff freigegeben ist, und klicken Sie auf **Daten verschlüsseln**.

Gehen Sie folgendermaßen vor, um die Daten über das Kontextmenü zu entschlüsseln:

1. Öffnen Sie durch Rechtsklick das Kontextmenü der Containerdatei, der Verknüpfung für den Container (s. Abschnitt "Verknüpfung für den Container erstellen" auf S. 190) auf dem Desktop oder dem Wechseldatenträger.
2. Wählen Sie im folgenden Menü den Punkt **Daten verschlüsseln**.

DATEIEN ZU EINEM CONTAINER HINZUFÜGEN

Nachdem ein Container entsperrt (s. Abschnitt "Zugriff auf Daten in einem Container blockieren und freigeben" auf S. 188) wurde, wird er im System als virtueller Wechseldatenträger angezeigt und steht allen Benutzern des Betriebssystems zur Verfügung. Sie können einen Container öffnen und Dateien und Ordner, die in verschlüsselter Form gespeichert werden sollen, darin ablegen. Um die Sicherheit Ihrer Daten zu gewährleisten, müssen die Daten beim Abschluss der Arbeit verschlüsselt werden. Danach ist für den Zugriff auf verschlüsselte Daten, die sich in einem Container befinden, die Eingabe des Kennworts erforderlich.

Geben Sie folgendermaßen vor, um einen Container über die Programmoberfläche zu öffnen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Datenverschlüsselung**.
2. Wählen Sie im folgenden Fenster einen Container aus, auf den der Zugriff freigegeben ist, und öffnen Sie ihn durch Doppelklick.
3. Speichern Sie die Daten, die verschlüsselt werden sollen, in dem Container.

Gehen Sie folgendermaßen vor, um einen Container über das Kontextmenü zu öffnen:

1. Öffnen Sie durch Rechtsklick das Kontextmenü der Containerdatei oder der Verknüpfung für den Zugriff auf den Container (s. Abschnitt "Verknüpfung für den schnellen Zugriff auf einen Container erstellen" auf S. 190) auf dem Desktop.
2. Wählen Sie im folgenden Menü den Punkt **Container öffnen**.

EINSTELLUNGEN EINES CONTAINERS ANPASSEN

Sie können den Namen und das Zugriffskennwort eines Containers ändern.

Die Einstellungen können nur für einen Container geändert werden, auf den der Zugriff gesperrt ist.

Gehen Sie folgendermaßen vor, um einen Container umzubenennen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Datenverschlüsselung**.
2. Wählen Sie im folgenden Fenster einen Container und klicken Sie auf **Anpassen**.
3. Geben Sie im folgenden Fenster das Kennwort für den Zugriff auf den Container ein.
4. Geben Sie im folgenden Fenster **Parameter des Containers** einen neuen Namen für den Container an.

Gehen Sie folgendermaßen vor, um das Kennwort für den Zugriff auf einen Container zu ändern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Datenverschlüsselung**.
2. Wählen Sie im folgenden Fenster einen Container und klicken Sie auf **Anpassen**.
3. Geben Sie im folgenden Fenster das Kennwort für den Zugriff auf den Container ein.
4. Verwenden Sie im folgenden Fenster **Parameter des Containers** den Link **Kennwort ändern**.

5. Füllen Sie im folgenden Fenster **Kennwort ändern** alle Felder aus.

VERKNÜPFUNG FÜR DEN SCHNELLEN ZUGRIFF AUF EINEN CONTAINER ERSTELLEN

Für die bequeme Arbeit mit Daten kann auf dem Desktop eine Verknüpfung zum schnellen Zugriff auf einen Container erstellt werden. Mit dieser Verknüpfung können Sie den Container schnell öffnen sowie die Daten entschlüsseln und verschlüsseln, wobei der tatsächliche Ort der Containerdatei nebensächlich ist (falls von Ihrem Computer aus Zugriff auf diese Datei besteht). Eine Verknüpfung zum schnellen Zugriff kann beim Anlegen des Containers oder zu einem späteren Zeitpunkt erstellt werden.

Eine Verknüpfung kann nur für einen Container erstellt werden, auf den der Zugriff gesperrt ist.

Gehen Sie folgendermaßen vor, um eine Verknüpfung für den Zugriff auf einen Container zu erstellen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Datenverschlüsselung**.
2. Wählen Sie im folgenden Fenster einen Container aus und klicken Sie auf **Anpassen**.
3. Geben Sie im folgenden Fenster das Kennwort für den Zugriff auf den Container ein.
4. Klicken Sie im folgenden Fenster **Parameter des Containers** auf den Link **Verknüpfung auf Desktop erstellen**.

VERWALTUNG

Die Funktion Verwaltung dient dazu, das Programm Kaspersky PURE von einem Administratorarbeitsplatz aus auf den Computern eines Heimnetzwerks fernzuverwalten.

Über die Verwaltung kann ein Netzwerkadministrator folgende Aktionen ausführen:

- Schutzniveau der Computer im Netzwerk analysieren
- gesamtes Netzwerk und einzelne Computer auf die Existenz von Bedrohungen untersuchen
- Antiviren-Datenbanken zentral aktualisieren
- Parameter für den Schutz von Netzwerkcomputern anpassen
- Kindersicherung verwalten
- Backup der Daten auf Netzwerkcomputern ausführen
- Berichte über die Arbeit des Sicherheitssubsystems anzeigen

Gehen Sie folgendermaßen vor, um die Verwaltung zu starten:

Verwenden Sie im unteren Bereich des Hauptfensters von Kaspersky PURE den Link **Verwaltung**.

Beim ersten Start wird automatisch der Konfigurationsassistent für Remote-Administration (s. Abschnitt "Fernverwaltung anpassen" auf S. 191) gestartet. Bei späteren Starts ist die Eingabe des Administratorkennworts erforderlich.

Um das Programm auf den Computern eines Netzwerks fernzuverwalten, muss die Verwaltung auf allen Computern durch das gleiche Administratorkennwort geschützt sein.

IN DIESEM ABSCHNITT

Fernverwaltung anpassen 191

Untersuchung eines Heimnetzwerks auf Viren und Schwachstellen 192

Remote-Update der Datenbanken auf Netzwerkcomputern 192

Schutzkomponenten auf Netzwerkcomputern aktivieren / deaktivieren 193

Kindersicherung fernverwalten 193

Backup auf Netzwerkcomputern starten 194

Remote-Verwaltung von Lizenzen auf Netzwerkcomputern 194

FERNVERWALTUNG ANPASSEN

Die Fernverwaltung wird mit Hilfe eines Assistenten angepasst. Beim ersten Start der Verwaltung wird automatisch der Konfigurationsassistent gestartet. Künftig kann der Assistent manuell gestartet werden.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**, zum Abschluss des Assistenten die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf **Abbrechen** beendet werden.

Außerdem können Sie mit Hilfe der Schaltflächen im oberen Fensterbereich zwischen den einzelnen Schritten des Assistenten navigieren.

Gehen Sie folgendermaßen vor, um die Parameter für die Verwaltung anzupassen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im unteren Bereich des Fensters auf **Verwaltung**.
2. Klicken Sie im folgenden Fenster oben auf den Link **Einstellungen**, um den Konfigurationsassistenten zur Remote-Verwaltung zu starten. Details zu den einzelnen Schritte des Assistenten:
   a. Geben Sie im Fenster **Kennwortschutz** das Administratorkennwort ein oder ändern Sie es.
   b. Wählen Sie im Fenster **Computer suchen** die Computer für die Fernverwaltung aus.
   c. Wählen Sie im Fenster **Updatemethode** eine Methode für das Update der Datenbanken aus
   d. Bestätigen Sie im Fenster **Übersicht** die ausgewählten Parameter.

UNTERSUCHUNG EINES HEIMNETZWERKS AUF VIREN UND SCHWACHSTELLEN

Über die Verwaltung können Sie im Remote-Modus eine Aufgabe zur Virensuche für das gesamte Netzwerk oder für einen einzelnen Computer starten.

Gehen Sie folgendermaßen vor, um das gesamte Netzwerk auf Viren zu untersuchen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im unteren Bereich des Fensters auf **Verwaltung**.
2. Klicken Sie im folgenden Fenster im Block **Aktionen für Netzwerk** oben auf den Link **Virensuche ausführen**.
3. Wählen Sie im folgenden Fenster **Gruppenweiser Start der Untersuchung** den Untersuchungstyp und die zu untersuchenden Computer.

Gehen Sie folgendermaßen vor, um einen einzelnen Computer auf Viren und Schwachstellen zu untersuchen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Verwaltung** im oberen Fensterbereich.
2. Wählen Sie im oberen Bereich des folgenden Fensters einen Computer und gehen Sie zum Abschnitt **Untersuchung**.
3. Wählen Sie auf der rechten Fensterseite die erforderliche Untersuchungsaufgabe.

REMOTE-UPDATE DER DATENBANKEN AUF NETZWERKCOMPUTERN

Mit der Verwaltung können Sie das Update von Kaspersky PURE auf den Netzwerkcomputern fernverwalten.

Folgende Updatemethoden stehen zur Auswahl:

- Datenbanken auf Computern unabhängig voneinander aktualisieren
- Update-Download von einem ausgewählten Computer im Netzwerk. Dabei muss ein Netzwerkcomputer als Updateserver festgelegt werden. Die übrigen Computer laden die Updates von diesem Computer herunter.

Gehen Sie folgendermaßen vor, um die Methode zum Update der Datenbanken für die Computer im Netzwerk zu ändern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Verwaltung** im oberen Fensterbereich.

2. Klicken Sie im oberen Bereich des folgenden Fensters auf den Link **Einstellungen**.

3. Der Konfigurationsassistent für die Verwaltung wird geöffnet. Gehen Sie dort zum Schritt **Updatemethode** und wählen Sie die entsprechende Updatemethode aus.

Gehen Sie folgendermaßen vor, um einen Computer als Updateserver festzulegen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im unteren Bereich des Fensters auf **Verwaltung**.

2. Wählen Sie im oberen Bereich des folgenden Fensters einen Computer und und gehen Sie zum Abschnitt **Update**.

3. Klicken Sie auf **Als Updateserver festlegen**.

Über die Verwaltung können Sie im Remote-Modus eine Updateaufgabe für das gesamte Netzwerk oder für einen einzelnen Computer starten.

Gehen Sie folgendermaßen vor, um das Update auf allen Netzwerkcomputern zu starten:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf**Verwaltung** im oberen Fensterbereich.

2. Klicken Sie im oberen Bereich des folgenden Fensters im Menü **Aktionen für Netzwerk** auf den Link **Update ausführen**.

3. Wählen Sie im folgenden Fenster **Gruppenweiser Start des Updates** die Computer, die aktualisiert werden sollen.

Gehen Sie folgendermaßen vor, um das Update auf einem einzelnen Computer zu starten:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Verwaltung** im oberen Fensterbereich.

2. Wählen Sie im oberen Bereich des folgenden Fensters einen Computer und und gehen Sie zum Abschnitt **Update**.

3. Klicken Sie auf der rechten Fensterseite auf **Update ausführen**.

SCHUTZKOMPONENTEN AUF NETZWERKCOMPUTERN AKTIVIEREN / DEAKTIVIEREN

Über die Verwaltung können Sie ferngesteuert die einzelnen Schutzkomponenten auf den Netzwerkcomputern aktivieren / deaktivieren.

Gehen Sie folgendermaßen vor, um eine Schutzkomponente ferngesteuert zu aktivieren/deaktivieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Verwaltung** im oberen Fensterbereich.

2. Wählen Sie im folgenden Fenster den Computer, dessen Schutz verwaltet werden soll, und gehen Sie zum Abschnitt **Informationen**.

3. Wählen Sie im rechten Fensterbereich den Punkt **Schutzkomponenten**.

4. Aktivieren / deaktivieren Sie im folgenden Fenster **Schutzkomponenten** die entsprechende Schutzkomponente durch Klick auf das Statussymbol rechts vom Namen der Komponente.

KINDERSICHERUNG FERNVERWALTEN

Über die Verwaltung können Sie im Remote-Modus Begrenzungen festlegen und eine Statistik der Ereignisse anzeigen, die mit der Arbeit von Benutzern auf den Netzwerkcomputern und im Internet zusammenhängen.

- *Gehen Sie folgendermaßen vor, um die Kindersicherung ferngesteuert anzupassen:*

  1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Verwaltung** im oberen Fensterbereich.
  2. Wählen Sie im oberen Bereich des folgenden Fensters einen Computer und gehen Sie zum Abschnitt **Kindersicherung**.
  3. Wählen Sie auf der rechten Fensterseite ein Benutzerkonto und klicken Sie auf **Anpassen**.

- *Gehen Sie folgendermaßen vor, um eine Statistik anzuzeigen:*

  1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Verwaltung** im oberen Fensterbereich.
  2. Wählen Sie im oberen Bereich des folgenden Fensters einen Computer und gehen Sie zum Abschnitt **Kindersicherung**.
  3. Wählen Sie auf der rechten Fensterseite ein Benutzerkonto und klicken Sie auf **Detaillierter Bericht**.

BACKUP AUF NETZWERKCOMPUTERN STARTEN

Über die Verwaltung können Sie im Remote-Modus Backup-Aufgaben auf Netzwerkcomputern ausführen und einen Bericht über die Ausführung von Aufgaben zum Backup und zur Datenwiederherstellung anzeigen.

- *Gehen Sie folgendermaßen vor, um das Backup im Remote-Modus zu verwalten:*

  1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Verwaltung** im oberen Fensterbereich.
  2. Wählen Sie im oberen Bereich des folgenden Fensters einen Computer und gehen Sie zum Abschnitt **Backup**.
  3. Wählen Sie auf der rechten Fensterseite eine Backup-Aufgabe und klicken Sie auf **Ausführen**.

     Mit Hilfe der entsprechenden Schaltflächen im oberen Fensterbereich kann die Aufgabenausführung angehalten oder abgebrochen werden.

- *Gehen Sie folgendermaßen vor, um einen Bericht über Aufgaben zum Backup und zur Datenwiederherstellung zu erhalten:*

  1. Öffnen Sie das Programmhauptfenster und klicken Sie im unteren Bereich des Fensters auf **Verwaltung**.
  2. Wählen Sie im oberen Bereich des folgenden Fensters einen Computer und gehen Sie zum Abschnitt **Backup**.
  3. Klicken Sie im oberen Fensterbereich auf **Bericht anzeigen**.
  4. Passen Sie im folgenden Fenster **Bericht** die Darstellung der Ereignisinformationen an.

REMOTE-VERWALTUNG VON LIZENZEN AUF NETZWERKCOMPUTERN

Über die Verwaltung können Sie im Remote-Modus den Lizenzstatus auf den Netzwerkcomputern prüfen, die Gültigkeit einer Lizenz verlängern oder das Programm mit einer neuen Lizenz aktivieren.

- *Gehen Sie folgendermaßen vor, um die Lizenz auf einem Netzwerkcomputer zu verwalten:*

  1. Öffnen Sie das Programmhauptfenster und klicken Sie im unteren Bereich des Fensters auf **Verwaltung**.
  2. Wählen Sie im folgenden Fenster den Computer, für den eine Problemliste angezeigt werden soll, und gehen Sie zum Abschnitt **Informationen**.
  3. Wählen Sie auf der rechten Seite des folgenden Fensters den Punkt **Lizenzverwaltung**.
  4. Führen Sie im folgenden Fenster **Lizenzen verwalten** die entsprechenden Aktionen aus.

PASSWORD MANAGER

Password Manager speichert und schützt alle Ihre persönlichen Daten (z.B. Kennwörter, Benutzernamen, Nummern für Instant Messenger, Kontaktdaten, Telefonnummern usw.). Password Manager assoziiert Kennwörter und Benutzerkonten mit Programmen von Microsoft Windows oder mit Webseiten, für die sie verwendet werden. Alle Informationen werden in verschlüsselter Form in einer Kennwort-Datenbank gespeichert, auf die der Zugriff nur mit einem Master-Kennwort möglich ist. Ein Zugriff auf die Informationen ist nur möglich, wenn die Kennwort-Datenbank entsperrt ist. Nach dem Start einer Webseite oder eines Programms fügt Password Manager automatisch das Kennwort, den Benutzernamen und andere persönliche Daten ein. Somit ist es ausreichend, sich nur ein Kennwort zu merken und sich nicht alle Kennwörter einzuprägen.

In der Grundeinstellung wird Password Manager beim Hochfahren des Betriebssystems gestartet. Die Komponente wird in Programme integriert, wodurch erlaubt wird, persönliche Daten direkt aus einem Programmfenster zu verwalten.

Password Manager verfolgt die Aktionen, die Programme mit Kennwörtern ausführen, und verhindert das Abfangen und den Diebstahl persönlicher Informationen. Die Komponente untersucht Programme, die Kennwörter verwenden oder von anderen Programmen ein Kennwort abfragen, und bietet Ihnen anschließend an, eine verdächtige Aktion zu erlauben oder zu verbieten.

Außerdem bietet Password Manager folgende Möglichkeiten:

- Speicherung und Verwendung Ihrer Kennwörter (s. S. 205).
- Suche nach Benutzerkonten, Kennwörtern, Benutzernamen und anderen persönlichen Informationen in der Kennwort-Datenbank (s. S. 205).
- Generieren von zuverlässigen Kennwörtern (s. S. 223), wenn neue Benutzerkonten eingerichtet werden.
- Speicherung aller Kennwörter auf einem Wechseldatenträger (s. S. 224).
- Wiederherstellung der Kennwort-Datenbank aus einer Sicherungskopie (s. S. 208).
- Schutz der Kennwörter vor unerlaubtem Zugriff (s. S. 196).

Um den Password Manager aus dem Hauptfenster von Kaspersky PURE zu öffnen,

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.

Um den Password Manager aus dem Kontextmenü zu öffnen,

wählen Sie im Kontextmenü des Password Managers den Punkt **Password Manager**.

Außerdem können Sie festlegen, dass der Password Manager durch Doppelklick (s. S. 223) auf das Symbol des Password Managers im Infobereich der Taskleiste gestartet wird.

IN DIESEM ABSCHNITT

Kennwort-Datenbank verwalten 196

Programmparameter anpassen 210

Erstellen von sicheren Kennwörtern 223

Verwendung einer portablen Version des Password Managers 224

KENNWORT-DATENBANK VERWALTEN

In der Kennwort-Datenbank sind alle Benutzerkonten für Programme und Web-Seiten mit einem oder mehreren Benutzernamen gespeichert. Außerdem enthält sie Visitenkarten (die z.B. Kontaktdaten, Telefonnummern, Nummern von Instant Messengern usw. enthalten).

Die Arbeit mit der Kennwort-Datenbank ist nur möglich, wenn sie nicht blockiert ist (s. S. 196). Bevor die Kennwort-Datenbank verändert wird, sollten die Parameter für das Backup der Datenbank (s. S. 216) angepasst werden. Wenn die Daten versehentlich verändert oder gelöscht wurden, verwenden Sie die Wiederherstellung der Kennwort-Datenbank (s. S. 208).

Sie können folgende Aktionen ausführen:

- persönliche Daten hinzufügen (s. S. 197), ändern und löschen (s. S. 206).
- Kennwort-Datenbank importieren / exportieren (s. S. 206) oder wiederherstellen (s. S. 208).

IN DIESEM ABSCHNITT

Zugriff auf die Kennwort-Datenbank 196

Persönliche Daten hinzufügen 197

Persönliche Daten verwenden 205

Kennwörter suchen 205

Persönliche Daten löschen 206

Daten importieren/exportieren 206

Backup / Wiederherstellung der Kennwort-Datenbank 208

ZUGRIFF AUF DIE KENNWORT-DATENBANK

Für den Zugriff auf die Kennwort-Datenbank kann eine der folgenden Authentifizierungsmethode ausgewählt werden.

- **Schutz durch ein Master-Kennwort**. Für den Zugriff auf die Kennwort-Datenbank wird ein Master-Kennwort verwendet.
- **USB-Gerät**. Für den Zugriff auf die Kennwort-Datenbank wird ein Gerät mit USB-Interface verwendet, das an den Computer angeschlossen wird. Wenn das USB-Gerät getrennt wird, wird die Kennwort-Datenbank automatisch blockiert.
- **Bluetooth-Gerät**. Für den Zugriff auf die Kennwort-Datenbank wird ein Bluetooth-Gerät verwendet, das an Ihren Computer angeschlossen wird. Wenn das Bluetooth-Gerät getrennt wird, wird die Kennwort-Datenbank automatisch blockiert.
- **Ohne Authentifizierung**. Der Zugriff auf die Kennwort-Datenbank ist nicht geschützt.

In der Grundeinstellung ist der Schutz durch ein Master-Kennwort eingestellt, womit es ausreichend ist, sich nur ein Kennwort zu merken, und sich nicht alle Kennwörter einzuprägen.

Das Master-Kennwort ist eine wichtige Methode für den Schutz Ihrer persönlichen Daten. Wenn als Authentifizierungsmethode ein Gerät ausgewählt wurde und dieses Gerät nicht verfügbar ist (oder z.B. verloren wurde), können Sie das Master-Kennwort verwenden, um auf Ihre persönlichen Daten zuzugreifen.

In der Grundeinstellung blockiert Password Manager die Kennwort-Datenbank beim Programmstart und nachdem der Computer für einen bestimmten Zeitraum inaktiv war (s. S. 218). Die Arbeit mit dem Programm ist nur möglich, wenn die Kennwort-Datenbank nicht blockiert ist.

Sie können die Kennwort-Datenbank auch auf folgende Arten freigeben / blockieren:

- im Fenster Password Manager (s. S. 52).
- mit einem USB- oder Bluetooth-Gerät – wird nur für die Authentifizierungsmethode mit einem USB- oder Bluetooth-Gerät verwendet.
- durch Doppelklick auf das Programmsymbol (s. S. 223) – Dafür muss zusätzlich die Aktion bei Doppelklick festgelegt werden.
- aus dem Kontextmenü von Password Manager (s. S. 53).
- mit der Tastenkombination STRG+ALT+L (s. S. 214).

Zur Eingabe des Master-Kennworts können Sie die virtuelle Tastatur verwenden, mit der Kennwörter ohne die herkömmliche Tastatur eingegeben werden können.

Gehen Sie folgendermaßen vor, um das Programm aus dem Kontextmenü des Programms zu blockieren:

1. Klicken Sie im Infobereich der Taskleiste mit der rechten Maustaste auf das Symbol von Password Manager.
2. Wählen Sie im folgenden Menü den Punkt **Blockieren**.

Gehen Sie folgendermaßen vor, um die Kennwort-Datenbank aus dem Kontextmenü freizugeben:

1. Klicken Sie im Infobereich der Taskleiste mit der rechten Maustaste auf das Programmsymbol von Password Manager.
2. Wählen Sie im folgenden Menü den Punkt **Freigeben**.
3. Geben Sie im folgenden Fenster das Master-Kennwort ein.

PERSÖNLICHE DATEN HINZUFÜGEN

Persönliche Daten können nur hinzugefügt werden, wenn die Kennwort-Datenbank nicht blockiert ist (s. S. 196). Ein neues Benutzerkonto wird beim Start eines Programms / einer Webseite automatisch erkannt, wenn es nicht in der Kennwort-Datenbank gefunden wurde. Nach der Authentifizierung in einem Programm / auf einer Webseite schlägt Password Manager dann vor, die persönlichen Daten zur Kennwort-Datenbank hinzuzufügen.

In der Kennwort-Datenbank werden folgende Typen von persönlichen Daten unterschieden:

- **Benutzerkonto**. Kombination aus Benutzernamen und Kennwort für die Authentifizierung auf einer Webseite oder in einem Programm.
- **Gruppe von Benutzerkonten**. Sie dienen der bequemen Organisation von Benutzerkonten in der Kennwort-Datenbank.
- **Benutzername**. Password Manager schlägt in der Grundeinstellung vor, ein Benutzerkonto mit einem Benutzernamen zu erstellen. Ein zusätzlicher Benutzername wird verwendet, wenn Programme oder Webseiten es erlauben, mehrere Benutzernamen für den Zugriff auf ihre Ressourcen anzulegen.
- **Visitenkarte**. Sie dienen zum Speichern von Daten wie Geschlecht, Geburtsdatum, Kontaktinformationen, Telefonnummer, Arbeitsplatz, Nummer eines Instant Messengers, Homepage-Adresse usw. Um geschäftliche und private Informationen zu trennen, können Sie mehrere Visitenkarten anlegen.
- **Persönliche Notiz**. Dient zum Speichern beliebiger Informationen.

BENUTZERKONTO

Password Manager erkennt ein neues Benutzerkonto automatisch, wenn es nicht in der Kennwort-Datenbank gefunden wurde. Nach Abschluss der Authentifizierung in einem Programm / auf einer Webseite schlägt Password Manager vor, die Daten in der Kennwort-Datenbank zu speichern. Sie können ein neues Benutzerkonto auch manuell zur Kennwort-Datenbank hinfügen.

Ein Benutzerkonto enthält folgende Daten:

- Typ des Benutzerkontos (Benutzerkonto für ein Programm oder Benutzerkonto für das Internet)
- Benutzername / mehrere Benutzername
- Kennwort
- Pfad des Programms / Webadresse der Webseite im Internet (abhängig vom Typ des Benutzerkontos)
- Einstellungen für die Assoziation des Benutzerkontos mit einem Objekt
- Einstellungen für die Aktivierung des Benutzerkontos
- Kommentar
- Einstellungen für das Ausfüllen zusätzlicher Felder auf einer Webseite

Password Manager erlaubt es, ein oder mehrere Benutzerkonten für die Authentifizierung in einem Programm oder auf einer Webseite zu verwenden.

Auf Basis des Pfads für ein Programm oder der Webadresse für eine Webseite kann mit Hilfe von Password Manager ein Bereich für die Verwendung eines Benutzerkontos festgelegt werden.

Es bestehen folgende Möglichkeiten, um ein Benutzerkonto hinzuzufügen:

- Titelleisten-Schaltfläche – Dazu wird im Menü der Titelleisten-Schaltfläche der Punkt **Benutzerkonto hinzufügen** ausgewählt.
- aus dem Kontextmenü von Password Manager – Dazu dient der Punkt **Benutzerkonto hinzufügen** im Kontextmenü von Password Manager.
- aus dem Hauptfenster von Password Manager

Gehen Sie folgendermaßen vor, um vom Hauptfenster aus ein neues Benutzerkonto hinzuzufügen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Password Manager** auf **Kennwort-Datenbank**.
4. Klicken Sie im folgenden Fenster oben auf **Hinzufügen** und wählen Sie den Punkt **Benutzerkonto hinzufügen**.
5. Wählen Sie im folgenden Assistentenfenster einen Typ für das Benutzerkonto aus (Benutzerkonto für das Internet, Benutzerkonto für ein Programm oder benutzerdefinierter Modus) und klicken Sie auf **Weiter**.
   - Wenn Sie ein Benutzerkonto für das Internet oder für ein Programm ausgewählt haben, geben Sie eine Webseite oder ein Programm an, für das dieses Benutzerkonto dienen soll, und klicken Sie auf **Weiter**.
   - Wenn Sie den erweiterten Modus ausgewählte haben, geben Sie auf der Registerkarte **Assoziation** einen Programmpfad / eine Webseite an und passen Sie die Verwendung des Benutzerkontos an.
6. Geben Sie im oberen Fensterbereich im Feld **Name** einen Namen für das neue Benutzerkonto ein oder ändern Sie den Namen.

7. Geben Sie auf der Registerkarte **Zugangsdaten** den Benutzernamen und das Kennwort an.

   Ein Benutzername kann aus einem oder mehreren Wörtern bestehen. Um für einen Benutzernamen Schlüsselwörter festzulegen (s. S. 199) klicken Sie auf die Schaltfläche .

   Um einen Benutzernamen / ein Kennwort in die Zwischenablage zu kopieren, klicken Sie auf .

   Um einen Benutzernamen aus einem anderen Benutzerkonto zu kopieren, verwenden Sie den Link **Benutzername eines anderen Benutzerkontos verwenden**.

   Um automatisch ein neues Kennwort zu erstellen, klicken Sie auf den Link **Neues Kennwort generieren** (s. S. 223).

8. Passen Sie bei Bedarf auf der Registerkarte **Formular manuell ändern** die Parameter für das Ausfüllen von anderen Feldern auf einer Webseite an.

9. Geben Sie bei Bedarf auf der Registerkarte **Kommentar** eine Erläuterung für das Benutzerkonto an. Damit der Kommentar nach der Aktivierung des Benutzerkontos in einer Meldung erscheint, aktivieren Sie das Kontrollkästchen **Kommentare in Meldung anzeigen**.

SCHLÜSSELWÖRTER FÜR DIE SUCHE FESTLEGEN

Zur schnellen Suche nach persönlichen Daten in der Kennwort-Datenbank können Schlüsselwörter verwendet werden. Sie werden für jeden Benutzernamen angelegt. Es wird empfohlen, die Schlüsselwörter beim Hinzufügen eines Benutzerkontos (s. S. 198) / Benutzernamens (s. S. 203) festzulegen.

Gehen Sie folgendermaßen vor, um Schlüsselwörter für einen Benutzernamen festzulegen:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.

3. Klicken Sie im folgenden Fenster **Password Manager** auf **Kennwort-Datenbank**.

4. Wählen Sie einen Benutzernamen aus der Liste **Meine Kennwörter** aus und klicken Sie im oberen Fensterbereich auf **Ändern**.

5. Klicken Sie im folgenden Fenster auf die Schaltfläche neben dem Feld **Benutzername** und geben Sie im Feld **Beschreibung** die Schlüsselwörter ein.

   Wenn ein Benutzerkonto mit einem Benutzernamen ausgewählt wurde, klicken Sie im folgenden Fenster **Benutzerkonto mit einem Benutzernamen** auf der Registerkarte **Zugangsdaten** auf die Schaltfläche .

PFAD EINES PROGRAMMS/ EINER WEBSEITE HINZUFÜGEN

Um ein Benutzerkonto mit einem Programm oder einer Webseite zu assoziieren, muss ein Link erstellt werden. Für eine Webseite besteht der Link aus einer Webadresse, für ein Programm aus dem Pfad einer ausführbaren Programmdatei auf dem Computer. Ohne diese Angaben wird ein Benutzerkonto nicht mit einem Programm / einer Webseite verknüpft.

Es gibt folgende Methoden, um ein Programm / eine Webseite mit einem Benutzerkonto zu verknüpfen:

- Mit der Schaltfläche wird ein Link aus der Liste der ausgewählten Webseiten Ihres Webbrowsers oder aus der Liste der Programme auf Ihrem Computer ausgewählt.
- manuelle Angabe des Pfads eines Programms / einer Webseite
- Verwendung von Password Manager

Um die Korrektheit eines eingegebenen Pfads zu prüfen, starten Sie das Programm / die Webseite mit der Schaltfläche .

Gehen Sie folgendermaßen vor, um einen Link aus der Liste auszuwählen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Password Manager** auf **Kennwort-Datenbank**.
4. Klicken Sie im oberen Fensterbereich auf **Hinzufügen** und wählen Sie den Punkt **Benutzerkonto hinzufügen**.
5. Klicken Sie im folgenden Fenster auf der Registerkarte **Links** im Feld **Link** auf die Schaltfläche .
6. Geben Sie im folgenden Fenster im Feld **Link** den Pfad für das Programm / für die Webseite an.

   Um eine Webseite aus der Liste der gespeicherten Webseiten (Lesezeichen) anzugeben, wählen Sie die Webseite in der Liste **Lesezeichen** aus und klicken Sie auf den Link **Link aus Favoriten kopieren**. Um den Pfad einer Webseite aus dem Browserfenster zu kopieren, klicken Sie auf den Link **Pfad des verknüpften Programms verwenden**.

   Um einen Link zu einem Programm zu erstellen, klicken Sie im Feld **Link** auf und geben Sie den Pfad der ausführbaren Programmdatei an.

Gehen Sie folgendermaßen vor, um den Pfad eines Programms / einer Webseite manuell anzugeben:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Password Manager** auf **Kennwort-Datenbank**.
4. Klicken Sie im oberen Fensterbereich auf **Hinzufügen** und wählen Sie den Punkt **Benutzerkonto hinzufügen**.
5. Geben Sie im folgenden Fenster auf der Registerkarte **Links** im Feld **Link** den Pfad des Programms / die Adresse der Webseite an. Die Adresse einer Webseite muss mit http://www beginnen.

Gehen Sie folgendermaßen vor, um den Pfad eines Programms / einer Webseite mit dem Zeiger von Password Manager anzugeben:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Password Manager** auf **Kennwort-Datenbank**.
4. Klicken Sie im oberen Fensterbereich auf **Hinzufügen** und wählen Sie den Punkt **Benutzerkonto hinzufügen**.
5. Geben Sie im folgenden Fenster auf der Registerkarte **Links** im Feld **Link** den Pfad des Programms / der Webseite an. Führen Sie dazu den Zeiger von Password Manager in das Fenster des Programms / des Webbrowsers.

METHODE FÜR DIE VERKNÜPFUNG EINES BENUTZERKONTOS AUSWÄHLEN

Um zu ermitteln, aus welchem Benutzerkonto beim Start eines Programms / einer Webseite automatisch Daten eingetragen werden sollen, verwendet Password Manager den Pfad eines Programms / die Webadresse einer Webseite.

Da Password Manager es erlaubt, mehrere Benutzerkonten für ein Programm / eine Webseite zu verwenden, ist es erforderlich, für jedes Benutzerkonto einen Verwendungsbereich festzulegen.

Auf Basis des Pfads für ein Programm / der Webadresse für eine Webseite kann mit Hilfe von Password Manager ein Bereich für die Verwendung eines Benutzerkontos festgelegt werden. Die Parameter für den Bereich werden beim Erstellen eines Benutzerkontos (s. S. 198) angepasst. Diese Werte können später geändert werden.

Die Varianten für die Verwendung eines Benutzerkontos unterscheiden sich in Abhängigkeit des Objekts (Programm oder Webseite).

Für ein Programm bestehen folgende Varianten:

- Benutzerkonto für ein Programm verwenden. Das Benutzerkonto wird für alle Programmfenster verwendet, die Eingabefelder für persönliche Daten besitzen.

- Nach Fenstertitel erkennen. Das Benutzerkonto wird nur für das angegebene Fenster des Programms verwendet.

  Ein Programm kann beispielsweise mehrere Benutzerkonten verwenden. Für die einzelnen Benutzerkonten unterscheiden sich in einem Programm nur die Fenstertitel. Password Manager trägt auf Basis des Titels eines Programmfensters automatisch die Daten eines Benutzerkontos ein.

Für Webseiten bestehen folgende Varianten für die Verwendung eines Benutzerkontos:

- Nur für die angegebene Webseite. Benutzername und Kennwort werden von Password Manager nur auf der Webseite mit der angegebenen Adresse automatisch in die Authentifizierungsfelder eingefügt.

  Wenn ein Benutzerkonto beispielsweise mit einer Webseite der Adresse http://www.web-site.com/login.html verknüpft ist, gilt dieses Benutzerkonto nicht für andere Webseiten dieser Webseite (z.B. für http://www.web-site.com/index.php).

- Für Webseiten aus einem Ordner. Password Manager fügt Benutzername und Kennwort automatisch in die Authentifizierungsfelder für alle Webseiten des letzten Ordners ein.

  Wenn beispielsweise die Adresse der Webseite http://www.web-site.com/cgi-bin/login.html eingegeben wurde, wird dieses Benutzerkonto für alle Webseiten im Ordner *cgi-bin* verwendet.

- Für eine Webseite: <Domänenname ab Third Level oder niedriger>. Dieses Benutzerkonto wird für eine beliebige Webseite der Domäne verwendet (: <ab Third-Level-Domain oder niedriger>.

  Password Manager fügt beispielsweise automatisch die Zugangsdaten für folgende Webseiten ein: http://www.domain1,domain2,web-site.com/login.html oder http://www.domain1,domain2,web-site.com/index.php. Dieses Benutzerkonto wird allerdings nicht verwendet für Webseiten mit Adressen, die verschiedene Fourth-Level-Domains besitzen: http://www.domain3.domain2.web-site.com/index.php oder http://www.domain4.domain2.web-site.com/index.php.

- Für eine Webseite: <Name der Webseite>. Dieses Benutzerkonto wird für alle Seiten einer Webseite verwendet, die Eingabefelder für Benutzername und Kennwort besitzen.

  Password Manager fügt beispielsweise automatisch die Zugangsdaten für folgende Webseiten ein: http://www.domain1,domain2,web-site.com/login.html, http://www.domain2,domain2,web-site.com/index.php, http://www.domain3,domain2,web-site.com/index.php oder http://www.domain4,domain2,web-site.com/index.php.

Gehen Sie folgendermaßen vor, um die Parameter für die Verwendung eines Benutzerkontos festzulegen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Password Manager** auf **Kennwort-Datenbank**.
4. Wählen Sie ein Benutzerkonto aus der Liste **Meine Kennwörter** aus und klicken Sie auf **Ändern**.
5. Wählen Sie im folgenden Fenster auf der Registerkarte **Links** eine Variante für die Verwendung des Benutzerkontos.

BENUTZERKONTO AUTOMATISCH AKTIVIEREN

Die automatische Aktivierung eines Benutzerkontos ist standardmäßig aktiviert. Password Manager fügt nur Benutzername und Kennwort in die Authentifizierungsfelder ein. Sie können die Aktivierungsparameter eines Benutzerkontos anpassen (s. S. 198).

Für Webseiten wird zusätzlich der Bereich der Webadressen angegeben, für den die automatische Aktivierung verwendet werden soll.

Es bestehen folgende Varianten für die Aktivierung eines Benutzerkontos:

- Nur für eine angegebene Webseite. Das Benutzerkonto wird nur für diese Webseite aktiviert.
- Für eine Webseite. Das Benutzerkonto wird für alle Webseiten einer Webseite aktiviert.

Gehen Sie folgendermaßen vor, um die automatische Aktivierung eines Benutzerkontos festzulegen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Password Manager** auf **Kennwort-Datenbank**.
4. Wählen Sie ein Benutzerkonto aus der Liste **Meine Kennwörter** aus und klicken Sie auf **Ändern**.
5. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Links** das Kontrollkästchen **Benutzerkonto nach dem Laden automatisch aktivieren**.

   Wählen Sie für eine Webseite zusätzlich eine Aktivierungsmethode für das Benutzerkonto.

ZUSATZFELDER AUSFÜLLEN

Bei der Authentifizierung auf einer Webseite werden neben Kennwort und Benutzername manchmal auch andere Daten abgefragt. Password Manager erlaubt es, Zusatzfelder automatisch auszufüllen. Sie können die Parameter für das automatische Ausfüllen von Zusatzfeldern für ein Benutzerkonto anpassen.

Die Parameter für Zusatzfelder können dann angepasst werden, wenn für ein Benutzerkonto der Pfad eines Programms / die Adresse einer Webseite angegeben ist.

Um die Parameter der Felder anzupassen, lädt Password Manager die Webseite vorübergehend und analysiert dann alle Felder und Schaltflächen. Felder und Schaltflächen werden für jede Webseite in Gruppen eingeteilt.

Während der Arbeit mit einer geladenen Webseite speichert Password Manager vorübergehend Dateien und Bilder auf Ihrem Computer.

Gehen Sie folgendermaßen vor, um die Parameter für Zusatzfelder anzupassen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Password Manager** auf **Kennwort-Datenbank**.
4. Wählen Sie ein Benutzerkonto aus der Liste **Meine Kennwörter** aus und klicken Sie auf **Ändern**.
5. Klicken Sie im folgenden Fenster auf der Registerkarte **Formular manuell ändern** auf den Link **Hier klicken, um die Werte der Felder zu ändern.**
6. Aktivieren Sie im folgenden Fenster **Formular manuell ändern** oben das Kontrollkästchen für das entsprechende Feld / Schaltfläche.
7. Aktivieren Sie durch Doppelklick das Feld in der Spalte **Wert** für ein ausgewähltes Feld / eine Schaltfläche.

GRUPPE FÜR BENUTZERKONTEN ERSTELLEN

Die Verwendung von Gruppen für Benutzerkonten ist hilfreich bei der Organisation von Informationen in der Kennwort-Datenbank. Eine Gruppe besteht aus einem Ordner, der hinzugefügte Benutzerkonten enthält.

Erstellte Gruppen werden im Kontextmenü von Password Manager angezeigt: Punkt **Benutzerkonten**-> **<Name der Gruppe>**.

Gehen Sie folgendermaßen vor, um eine Gruppe für Benutzerkonten zu erstellen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Password Manager** auf **Kennwort-Datenbank**.
4. Klicken Sie im oberen Fensterbereich auf **Hinzufügen** und wählen Sie den Punkt **Gruppe hinzufügen**.
5. Geben Sie einen Namen für die neue Gruppe ein.
6. Fügen Sie dem neuen Ordner Benutzerkonten aus der Liste **Meine Kennwörter** hinzu. Die Konten werden mit der Maus in den Ordner gezogen.

BENUTZERNAME

Für die Arbeit mit einigen Programmen / Webseiten werden häufig mehrere Benutzernamen verwendet. Password Manager erlaubt es, mehrere Benutzernamen für ein Benutzerkonto zu speichern. Password Manager erkennt einen neuen Benutzernamen automatisch bei der ersten Verwendung und schlägt vor, ihn zu dem Benutzerkonto für dieses Programm / diese Webseite hinzuzufügen. Sie können einen neuen Benutzernamen manuell für ein Benutzerkonto hinzufügen und ihn später ändern. Außerdem können Sie einen Benutzernamen für unterschiedliche Benutzerkonten verwenden.

Es bestehen folgende Möglichkeiten, um einen neuen Benutzernamen für ein Benutzerkonto hinzuzufügen:

- mit der Titelleisten-Schaltfläche. Wählen Sie dazu im Menü der Titelleisten-Schaltfläche den Punkt **Benutzerkonto ändern** –> **Benutzername hinzufügen**.
- aus dem Programmhauptfenster.

Gehen Sie folgendermaßen vor, um einen Benutzernamen für ein Benutzerkonto hinzuzufügen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Password Manager** auf **Kennwort-Datenbank**.
4. Wählen Sie ein Benutzerkonto aus der Liste **Meine Kennwörter** aus, klicken Sie auf **Hinzufügen** und wählen Sie den Punkt **Benutzername hinzufügen**.
5. Geben Sie im folgenden Fenster einen Benutzernamen und ein Kennwort ein. Ein Benutzername kann aus einem oder mehreren Wörtern bestehen. Um für einen Benutzernamen Schlüsselwörter festzulegen, klicken Sie auf die Schaltfläche und füllen Sie dann das Feld **Beschreibung** aus.

   Um einen Benutzernamen / ein Kennwort in die Zwischenablage zu kopieren, verwenden Sie die Schaltfläche . Um automatisch ein Kennwort zu erstellen, verwenden Sie den Link **Neues Kennwort generieren** (s. S. 223).

   Um einen Benutzernamen aus einem anderen Benutzerkonto zu kopieren, verwenden Sie den Link **Benutzername eines anderen Benutzerkontos verwenden**.

VISITENKARTE

Für die Anmeldung auf einer Webseite werden neben Benutzername und Kennwort häufig noch andere persönliche Daten verwendet (z.B. Vor- und Nachname, Geburtsjahr, Geschlecht, E-Mail-Adresse, Telefonnummer, Land u.a.). Password Manager erlaubt es, die gesamten Daten in Form von Visitenkarten in der verschlüsselten Kennwort-Datenbank zu speichern. Bei der Anmeldung auf einer neuen Webseite füllt Password Manager auf Grundlage der Daten aus einer ausgewählten Visitenkarte automatisch das Anmeldeformular aus. Um beim Speichern geschäftliche und private Informationen zu trennen, können mehrere Visitenkarten angelegt werden. Die Einstellungen einer Visitenkarte können später geändert werden.

Gehen Sie folgendermaßen vor, um eine Visitenkarte anzulegen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Password Manager** auf **Kennwort-Datenbank**.
4. Klicken Sie im oberen Fensterbereich auf **Visitenkarte hinzufügen**.
5. Geben Sie im folgenden Fenster im Feld **Name** einen Namen für die Visitenkarte an.
6. Geben Sie für die entsprechenden Felder einen Wert ein. Ein Feld wird durch Doppelklick auf die Spalte **Wert** aktiviert.

PERSÖNLICHE NOTIZ

Persönliche Notizen dienen dazu, Textinformationen in verschlüsselter Form zu speichern (z.B. Passdaten, Kontonummern usw.) und schnell auf die gespeicherten Daten zuzugreifen. Password Manager bietet eine Auswahl von Standardwerkzeugen zur Bearbeitung von persönlichen Notizen. Beim Erstellen einer persönlichen Notiz können Vorlagen mit einer Auswahl von standardmäßigen Datentypen (s. S. 220) verwendet werden.

Die Einstellungen für eine persönliche Notiz können später geändert werden.

Gehen Sie folgendermaßen vor, um eine persönliche Notiz ohne Vorlage zu erstellen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Password Manager** auf **Kennwort-Datenbank**.
4. Klicken Sie im oberen Fensterbereich auf **Persönliche Notiz hinzufügen**.
5. Geben Sie im folgenden Fenster im Feld **Name** einen Namen für die persönliche Notiz ein.
6. Geben Sie die entsprechenden Informationen im Texteditor ein.

Gehen Sie folgendermaßen vor, um eine persönliche Notiz auf Basis einer Vorlage zu erstellen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Password Manager** auf **Kennwort-Datenbank**.
4. Klicken Sie im oberen Fensterbereich auf **Persönliche Notiz hinzufügen**.
5. Geben Sie im folgenden Fenster im Feld **Name** einen Namen für die persönliche Notiz ein.
6. Klicken Sie im unteren Fensterbereich auf **Vorlage auswählen** und wählen Sie die entsprechende Vorlage aus.
7. Tragen Sie die erforderlichen Daten ein und formatieren Sie den Text entsprechend.

Um eine persönliche Notiz anzuzeigen,

öffnen Sie das Kontextmenü des Password Managers und wählen Sie den Punkt **Persönliche Notizen** → **<Name der Gruppe>** → **<Name der persönlichen Notiz>**.

PERSÖNLICHE DATEN VERWENDEN

Password Manager verknüpft Benutzerkonten mit Programmen / Webseiten, für die sie verwendet werden. Beim Start eines Programms / einer Webseite erfolgt in der Kennwort-Datenbank automatisch eine Suche nach einem verknüpften Benutzerkonto. Wenn ein Benutzerkonto gefunden wird, werden die persönlichen Daten automatisch eingetragen. Wenn die Kennwort-Datenbank kein verknüpftes Benutzerkonto enthält, schlägt Password Manager vor, es zur Kennwort-Datenbank hinzuzufügen (s. S. 198).

Einige Programme / Webseiten können mehrere Benutzernamen verwenden. Password Manager erlaubt es, mehrere Benutzernamen für ein Benutzerkonto zu speichern. Wenn bei der Authentifizierung ein neuer Benutzername verwendet wurde, schlägt der, Password Manager vor, ihn für das gestartete Programm / für die Webseite dem Benutzerkonto hinzuzufügen (s. S. 203). In diesem Fall erscheint beim Start eines Programms / einer Webseite neben den Eingabefeldern für persönliche Daten ein Fenster mit einer Liste der Benutzernamen für dieses Benutzerkonto.

Neben Benutzername und Kennwort werden für die Anmeldung auf einer Webseite häufig noch andere persönliche Daten verwendet (z.B. Vor- und Nachname, Geschlecht, Land, Stadt, Telefon, E-Mail-Adresse u.a.). Password Manager speichert solche Daten in Form von Visitenkarten in der verschlüsselten Kennwort-Datenbank. Um geschäftliche und private Informationen zu trennen, können Sie mehrere Visitenkarten anlegen (s. S. 204). Bei der Anmeldung in einem Programm / auf einer Webseite füllt Password Manager dann auf Grundlage der Daten aus einer ausgewählten Visitenkarte automatisch die Felder des Anmeldeformulars aus. Es ergibt sich eine Zeitersparnis, weil sich wiederholende Anmeldeformulare nicht manuell ausgefüllt werden müssen.

Bei der Authentifizierung in einem Programm / auf einer Webseite füllt Password Manager die persönlichen Daten nur dann aus, wenn die Kennwort-Datenbank nicht blockiert ist.

Ein Benutzerkonto kann auf folgende Arten verwendet werden:

- Programm / Webseite starten. Das Authentifizierungsformular wird auf Grundlage der Daten des Benutzerkontos automatisch ausgefüllt.
- Zeiger von Password Manager verwenden Führen Sie dazu den Cursor auf das Programmsymbol im Infobereich der Taskleiste und aktivieren Sie das Benutzerkonto anschließend, indem Sie den Zeiger von Password Manager in das Fenster des entsprechenden Programms / der Webseite ziehen.
- Benutzerkonto in der Liste der häufig verwendeten Benutzerkonten auswählen. Öffnen Sie dazu das Kontextmenü von Password Manager und wählen Sie im Block der häufig verwendeten Benutzerkonten einen Eintrag.
- Kontextmenü von Password Manager verwenden Öffnen Sie dazu das Kontextmenü des Kennwort-Managers und wählen Sie den Punkt **Benutzerkonten** – > **<Name des Benutzerkontos>**.

Gehen Sie folgendermaßen vor, um eine Visitenkarte zu verwenden:

1. Klicken Sie im Fenster des Programms / des Webbrowsers rechts oben auf die Titelleisten-Schaltfläche.
2. Wählen Sie im folgenden Menü den Punkt **Visitenkarten** – > **<Name der Visitenkarte>** aus. Password Manager füllt auf Grundlage der Daten aus der Visitenkarte automatisch die Anmeldefelder der Webseite aus.

KENNWÖRTER SUCHEN

Die Suche nach persönlichen Daten kann in folgenden Fällen erschwert werden:

- Bestimmte Kennwörter sind nicht mit Programmen / Webseiten verknüpft.
- Die Kennwort-Datenbank enthält eine große Anzahl von Benutzerkonten.

Mit Hilfe von Password Manager lassen sich Kennwörter schnell nach folgenden Parametern auffinden:

- Name des Benutzerkontos
- Benutzername
- Schlüsselwörter (s. S. 199) (Kriterien für Suche nach Schlüsselwörtern werden zusätzlich für jeden Benutzernamen eingestellt).
- Webadresse (für Webseiten)

Es kann nach einem gesamten Namen, nach Anfangsbuchstaben oder beliebigen Zeichen, die in dem Namen eines Benutzerkontos oder Links enthalten sind, gesucht werden.

Gehen Sie folgendermaßen vor, um ein Benutzerkonto zu suchen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Password Manager** auf **Kennwort-Datenbank**.
4. Geben Sie im oberen Fensterbereich in der Suchzeile einen Text ein.

PERSÖNLICHE DATEN LÖSCHEN

Bevor irgendwelche Änderungen von persönlichen Daten erfolgen, legt Password Manager automatisch eine Sicherungskopie der Kennwort-Datenbank an. Wenn die Daten versehentlich verändert oder gelöscht wurden, verwenden Sie die Wiederherstellung der Kennwort-Datenbank (s. S. 208). Es können ein oder alle Elemente aus der Kennwort-Datenbank gelöscht werden.

Gehen Sie folgendermaßen vor, um ein Element aus der Kennwort-Datenbank zu löschen:

1. Öffnen Sie Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Password Manager** auf **Kennwort-Datenbank**.
4. Wählen Sie ein Element aus der Liste **Meine Kennwörter** aus, klicken Sie auf **Löschen** und wählen Sie den Punkt **Löschen**.

Gehen Sie folgendermaßen vor, um alle Elemente aus der Kennwort-Datenbank zu löschen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Password Manager** auf **Kennwort-Datenbank**.
4. Wählen Sie ein Element aus der Liste **Meine Kennwörter** aus, klicken Sie auf **Löschen** und wählen Sie den Punkt **Alle löschen**.

DATEN IMPORTIEREN/EXPORTIEREN

Password Manager erlaubt den Import und Export Ihrer Kennwort-Datenbank sowie einzelner Objekte der Kennwort-Datenbank (Visitenkarten, Benutzerkonten oder persönliche Notizen).

Geladen werden können sowohl Kennwörter aus anderen Programmen zur Kennwort-Verwaltung (z.B. aus Internet Explorer, Mozilla Firefox, KeePass) als auch Kennwörter, die Sie früher mit Password Manager gespeichert haben. Der Import von Kennwörtern erfolgt aus Dateien der Formate xml und ini.

Password Manager erlaubt es, eine Kennwort-Datenbank in einer Datei des Formats xml, html oder txt zu speichern. Das Speichern eines Kennworts in einer Datei ist vorteilhaft, um den gemeinsamen Zugriff auf Kennwörter zu gewährleisten, um die Kennwort-Datenbank auszudrucken oder um eine Sicherungskopie der Kennwort-Datenbank in einem anderen Dateiformat (als dem Format von Password Manager) zu speichern.

Gespeicherte Kennwörter werden in unverschlüsselten Dateien gespeichert und sind nicht vor unerlaubtem Zugriff geschützt. Es wird deshalb empfohlen, rechtzeitig zu überlegen, wie die exportierten Daten geschützt werden können.

Die Kennwort-Datenbank wird beim Import verändert. Sie können auswählen, welche der folgenden Aktionen mit der Kennwort-Datenbank ausgeführt werden soll:

- **Überschreiben**. Die aktuelle Kennwort-Datenbank wird durch die geladene ersetzt (alle Kennwörter, die vor dem Laden in der Kennwort-Datenbank des Password Managers gespeichert waren, werden gelöscht).
- **Verbinden**. Die geladenen Kennwörter werden zur Kennwort-Datenbank hinzugefügt. Beim Zusammenführen können Sie auswählen, welche Benutzerkonten in den Password Manager geladen werden sollen.
- **Abbrechen**. Der Laden der Kennwörter wird abgebrochen.

Gehen Sie folgendermaßen vor, um Kennwörter aus einer Datei zu laden:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Password Manager** auf **Kennwort-Datenbank**.
4. Klicken Sie im unteren Bereich auf den Link **Kennwörter laden**.
5. Wählen Sie im folgenden Fenster **Kennwörter laden** das Programm, aus dem Kennwörter importiert werden sollen, und klicken Sie auf **Kennwörter laden**.
6. Geben Sie im folgenden Fenster die Datei mit Kennwörtern an, die Sie laden möchten, und klicken Sie auf **Öffnen**.
7. Wählen Sie im folgenden Fenster eine Aktion für die Kennwort-Datenbank aus.

Gehen Sie folgendermaßen vor, um die Kennwort-Datenbank in einer Datei zu speichern:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Password Manager** auf **Kennwort-Datenbank**.
4. Klicken Sie im unteren Bereich auf den Link **Kennwort speichern**.
5. Wählen Sie im folgenden Fenster eine Speicherungsmethode aus (Speicherung der gesamten Kennwort-Datenbank oder von ausgewählten Objekten) und klicken Sie auf **Weiter**.
6. Wählen Sie im folgenden Fenster die Speicherungseinstellungen aus.
   - Wenn Sie die zu speichernden Daten schützen möchten, wählen Sie die Variante **Sicheres Speichern** aus und legen Sie ein Kennwort für den Datenschutz fest.
   - Wenn Sie die Daten in einer unverschlüsselten Datei speichern möchten, wählen Sie die Variante **Unverschlüsseltes Speichern** aus und geben Sie ein Dateiformat für die Speicherung an.

- Um eine Änderung des Kennworts für die gespeicherten Daten zu planen, aktivieren Sie das Kontrollkästchen **Änderung des Kennworts für gespeicherte Objekte planen** und wählen Sie ein Datum aus, zu dem das Kennwort zurückgesetzt wird und Password Manager Sie darüber benachrichtigen soll, dass das Kennwort geändert werden muss.

7. Geben Sie im folgenden Fenster einen Pfad an, unter dem die Datei gespeichert werden soll, und klicken Sie auf **Weiter**.

8. Prüfen Sie im folgenden Fenster die Einstellungen für die Datenspeicherung und starten Sie den Speichervorgang.

BACKUP / WIEDERHERSTELLUNG DER KENNWORT-DATENBANK

Bevor irgendwelche Änderungen in der Kennwort-Datenbank erfolgen, wird automatisch eine Sicherungskopie angelegt. Der Pfad, unter dem die Sicherungskopien gespeichert werden, ist standardmäßig vorgegeben. Sie können ihn aber ändern (s. S. 216). Eine Wiederherstellung von Kennwörtern kann in folgenden Fällen von Nutzen sein:

- wenn vorherige Änderungen rückgängig gemacht werden sollen.
- wenn die Kennwort-Datenbank überschrieben oder gelöscht wurde.
- wenn die aktuelle Kennwort-Datenbank aufgrund eines Hardware- oder Systemfehlers nicht verfügbar / beschädigt ist.

Alle Daten eine Sicherungskopie werden in verschlüsselter Form gespeichert. Password Manager protokolliert alle Veränderungen in der Kennwort-Datenbank. Im Programm werden die Sicherungskopien nach Datum sortiert in einer Liste angezeigt, wobei die letzte Kopie an erster Stelle steht. Für jede Sicherungskopie werden folgende Daten genannt:

- Speicherort
- Datum und Uhrzeit der Erstellung
- Veränderungen im Vergleich zur vorhergehenden Version

Sicherungskopien können für folgende Aufgaben verwendet werden:

- Wiederherstellung der Kennwort-Datenbank aus einer ausgewählten Sicherungskopie
- Löschen alter Versionen von Sicherungskopien
- Ändern des Speicherorts für Sicherungskopien (s. S. 216).

➧ *Gehen Sie folgendermaßen vor, um die Kennwort-Datenbank wiederherzustellen:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Password Manager** auf **Kennwort-Datenbank**.
4. Klicken Sie im unteren Bereich des Fensters auf den Link **Kennwort-Datenbank wiederherstellen**.
5. Wählen Sie im folgenden Fenster **Wiederherstellung** das Datum einer Sicherungskopie aus der Liste aus und klicken Sie im oberen Fensterbereich auf **Wiederherstellen**.
6. Bestätigen Sie die Wiederherstellung im folgenden Fenster durch Klick auf **OK**.

➧ *Gehen Sie folgendermaßen vor, um nicht mehr benötigte Versionen von Sicherungskopien zu löschen:*

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.

3. Klicken Sie im folgenden Fenster **Password Manager** auf **Kennwort-Datenbank**.

4. Klicken Sie im unteren Bereich des Fensters auf den Link **Kennwort-Datenbank wiederherstellen**.

5. Wählen Sie im folgenden Fenster **Wiederherstellung** aus der Liste der Sicherungskopien jene Versionen, die gelöscht werden sollen. Halten Sie die Taste **STRG** gedrückt, um mehrere Versionen auszuwählen.

6. Klicken Sie auf **Löschen**.

7. Bestätigen Sie das Löschen der Sicherungskopien im folgenden Fenster durch Klick auf **OK**.

PROGRAMMPARAMETER ANPASSEN

Die Programmparameter können nur angepasst werden, wenn die Kennwort-Datenbank nicht blockiert ist (s. S. 196). Durch das Ändern der Parameter können Sie folgende Aktionen ausführen:

- Zeitpunkt für den Programmstart festlegen
- Meldungen aktivieren (s. S. 222).
- Benutzernamen festlegen (s. S. 211), der standardmäßig beim Erstellen eines neuen Benutzerkontos verwendet werden soll.
- Speicherdauer des Kennworts in der Zwischenablage festlegen (s. S. 222).
- Liste der häufig verwendeten Benutzerkonten anpassen (s. S. 212).
- Liste mit ignorierten Webseiten anlegen (s. S. 213), für die die Funktionen von Password Manager nicht verwendet werden.
- Liste mit vertrauenswürdigen Webseiten anlegen (s. S. 213), für die Password Manager eine Weiterleitung zulässt.
- Tastenkombinationen für den Schnellzugriff auf die Funktionen von Password Manager anpassen (s. S. 214).
- Speicherpfad für Kennwort-Datenbank (s. S. 214) und Sicherungskopien (s. S. 216) ändern.
- Methode zur Datenverschlüsselung ändern (s. S. 217).
- automatisches Blockieren der Kennwort-Datenbank anpassen (s. S. 218).
- Master-Kennwort ändern (s. S. 219).
- Zugriff auf die Kennwort-Datenbank anpassen (s. S. 218).
- Position der Titelleisten-schaltfläche ändern, Liste der Programme anlegen, die die Titelleisten-Schaltfläche unterstützen (s. S. 221).
- Liste der unterstützten Programme anlegen (s. S. 220).

Gehen Sie folgendermaßen vor, um die Funktionsparameter von Password Manager zu ändern:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Einstellungen**.
4. Wählen Sie im folgenden Fenster den Abschnitt aus, der geändert werden soll.
5. Nehmen Sie im rechten Fensterbereich für den ausgewählten Abschnitt die entsprechenden Änderungen vor.

IN DIESEM ABSCHNITT

Konfigurationsassistent 211

Standardmäßigen Benutzernamen verwenden 211

Häufig verwendete Benutzerkonten 212

Ignorierte Webadressen 213

Vertrauenswürdige Webadressen 213

Tastenkombination 214

Ort der Kennwort-Datenbank 214

Neue Kennwort-Datenbank anlegen 215

Speicherort für eine Sicherungskopie 216

Verschlüsselungsmethode auswählen 217

Kennwort-Datenbank automatisch blockieren 218

Authentifizierungsmethode für Password Manager ändern 218

USB- oder Bluetooth-Geräte zur Authentifizierung verwenden 219

Master-Kennwort ändern 219

Unterstützte Webbrowser 220

Vorlagen für persönliche Notizen verwalten 220

Titelleisten-Schaltfläche anzeigen 221

Speicherdauer des Kennworts in der Zwischenablage 222

Meldungen 222

Aktion bei Doppelklick 223

KONFIGURATIONSASSISTENT

Der Konfigurationsassistent für das Programm wird beim ersten Start von Password Manager gestartet. Seine Aufgabe besteht darin, Sie bei der ersten Konfiguration von Password Manager zu unterstützen. Dabei werden Ihre persönlichen Präferenzen und künftigen Aufgaben berücksichtigt.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**. Zum Abschluss des Assistenten dient die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf **Abbrechen** abgebrochen werden.

Im Folgenden werden die einzelnen Schritte des Konfigurationsassistenten beschrieben.

STANDARDMÄßIGEN BENUTZERNAMEN VERWENDEN

Password Manager erlaubt es, einen Benutzernamen festzulegen, der beim Erstellen eines neuen Benutzerkontos automatisch im Feld **Benutzername** angezeigt wird (s. S. 198).

Gehen Sie folgendermaßen vor, um einen standardmäßigen Benutzernamen festzulegen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Einstellungen**.
4. Wählen Sie im linken Bereich des folgenden Fensters den Abschnitt **Allgemein**.
5. Füllen Sie auf der Rechten Fensterseite das Feld **Standardmäßiger Benutzername** aus.

HÄUFIG VERWENDETE BENUTZERKONTEN

Password Manager ermöglicht den schnellen Zugriff auf Benutzerkonten. Eine Liste der häufig verwendeten Benutzerkonten wird im Programmhauptfenster angezeigt und kann außerdem im Kontextmenü und im Menü der Titelleisten-Schaltfläche angezeigt werden. Die Liste enthält die Namen der Programme / Webseiten, die Sie am häufigsten starten. Die Elemente dieser Liste sind alphabetisch oder nach Verwendungshäufigkeit angeordnet.

Die Liste der häufig verwendeten Benutzerkonten ist im Menü verfügbar, wenn die Kennwort-Datenbank nicht blockiert ist (s. S. 196).

Sie können folgende Parameter für die Liste festlegen:

- **Anzahl der Elemente in der Liste** – Maximale Anzahl der häufig verwendeten Benutzerkonten, die im Kontextmenü des Programms angezeigt werden sollen.
- **Liste im Programm-Menü anzeigen** – Die Liste der häufig verwendeten Benutzerkonten ist im Kontextmenü von Password Manager verfügbar.
- **Liste im Menü der der Titelleisten-Schaltfläche anzeigen** – Die Liste der häufig verwendeten Benutzerkonten ist im Menü der Titelleisten-Schaltfläche verfügbar (aus einem Programmfenster / Webbrowser).

Gehen Sie folgendermaßen vor, damit häufig verwendete Benutzerkonten im Kontexmenü angezeigt werden:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Einstellungen**.
4. Wählen Sie im linken Fensterbereichs den Abschnitt **Häufig verwendete Benutzerkonten**.
5. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Liste im Programm-Menü anzeigen**.

   Damit eine Liste der häufig verwendeten Benutzerkonten im Menü der Titelleisten-Schaltfläche angezeigt wird, aktivieren Sie das Kontrollkästchen **Im Menü der Titelleisten-Schaltfläche anzeigen**.

   Wenn das Kontrollkästchen **Liste im Programm-Menü anzeigen** deaktiviert ist, stehen die übrigen Parameter der Liste nicht für Änderungen zur Verfügung.

6. Geben Sie im Feld **Größe der Liste** die Anzahl der Benutzerkonten an.
7. Bei Bedarf können Sie die Liste manuell anpassen. Um ein Element aus der Liste zu löschen, markieren Sie darin das entsprechende Benutzerkonto und klicken Sie auf **Löschen**. Um alle Elemente aus der Liste zu löschen, klicken Sie auf **Leeren**.

IGNORIERTE WEBADRESSEN

Sie können eine Liste mit Webadressen anlegen, für die die Funktionen von Password Manager nicht verwendet werden. Für Webseiten aus dieser Liste wird die Funktion zum automatischen Ausfüllen von Kennwort und Benutzername deaktiviert. Außerdem schlägt Password Manager für diese Seiten nicht automatisch vor, ein neues Benutzerkonto (s. S. 198) / Benutzername zu (s. S. 203) erstellen.

Gehen Sie folgendermaßen vor, um eine Liste mit ignorierten Webadressen anzulegen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Einstellungen**.
4. Wählen Sie im linken Fensterbereich den Abschnitt **Ignorierte Webadressen**.
5. Klicken Sie auf der rechten Fensterseite auf **Hinzufügen**, geben Sie dann eine Webadresse ein und drücken Sie die **EINGABE**-Taste.

   Um eine Webadresse zu ändern, markieren Sie sie in der Liste und klicken Sie auf **Ändern**. Um eine Webadresse aus der Liste zu löschen, markieren Sie sie und klicken Sie auf **Löschen**.

VERTRAUENSWÜRDIGE WEBADRESSEN

Password Manager bietet Ihren persönlichen Daten Schutz vor Phishing-Attacken. Wenn Sie bei einem Authentifizierungsversuch auf eine andere Webseite umgeleitet werden, informiert das Programm Sie darüber.

Häufig verwenden Angreifer eine Weiterleitung auf Webseiten, die den Zugriff auf Bankkonten ermöglichen (es kann sich beispielsweise um Seiten von Internet-Banken, Zahlungssysteme usw. handeln). Auf der Authentifizierung der offiziellen Webseite einer Firma wird eine Weiterleitung auf eine gefälschte Webseite eingerichtet, die der offiziellen Internetseite visuell gleicht. Alle auf der gefälschten Seite eingegebenen Daten gelangen in die Hände der Angreifer.

Viele Webseiten enthalten ganz legale Weiterleitungen. Damit Password Manager eine solche Weiterleitung nicht als Phishing-Attacke bewertet, können Sie eine Liste mit vertrauenswürdigen Webadressen anlegen. In die Liste der vertrauenswürdigen Webadressen werden Webadressen eingetragen, an die eingegebene persönliche Daten weitergeleitet werden. Password Manager meldet nicht, wenn bei einer Authentifizierung persönliche Daten an eine vertrauenswürdige Webseite weitergeleitet werden.

Password Manager erlaubt die Weiterleitung persönlicher Daten von anderen Webseiten an eine vertrauenswürdige Webseite. Bevor Sie eine Webseite zur vertrauenswürdigen Liste hinzufügen, vergewissern Sie sich, dass sie vollkommen sicher ist.

Es bestehen folgende Möglichkeiten, um eine Webseite zur Liste der vertrauenswürdigen Webadressen hinzuzufügen:

- direkt bei der Authentifizierung auf einer Webseite
- manuell aus dem Fenster **Einstellungen von Password Manager**

Um eine Webseite während der Authentifizierung zur Liste der vertrauenswürdigen Webadressen hinzuzufügen, warten Sie auf die Weiterleitung zu einer anderen Webseite und aktivieren Sie im folgenden Fenster von Password Manager das Kontrollkästchen **<Name der Webseite> immer vertrauen**.

Gehen Sie folgendermaßen vor, um eine Liste mit vertrauenswürdigen Adressen manuell anzulegen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Einstellungen**.

4. Wählen Sie im linken Fensterbereich den Abschnitt **Vertrauenswürdige Webadressen**.

5. Klicken Sie auf der rechten Fensterseite auf **Hinzufügen**. In der Liste **Vertrauenswürdige Webadressen** wird ein Feld eingeblendet. Geben Sie die Webadresse ein und drücken Sie die **EINGABE**-Taste.

   Um eine Webadresse zu ändern, markieren Sie sie in der Liste und klicken Sie auf **Ändern**. Um eine Webadresse aus der Liste zu löschen, markieren Sie sie und klicken Sie auf **Löschen**.

TASTENKOMBINATION

Um schnell und bequem auf bestimmte Programmfunktionen zuzugreifen, können Tastenkombinationen verwendet werden.

Für folgende Aktionen können Tastenkombinationen festgelegt werden:

- Password Manager blockieren/freigeben (s. S. 196).
- Kennwort eingeben

Für einen schnellen Funktionsaufruf können eine Taste oder Kombination aus zwei oder drei Tasten festgelegt werden.

Vermeiden Sie es, den Funktionen des Password Managers die Tastenkombinationen zuzuweisen, die bereits für Microsoft Windows verwendet werden.

Gehen Sie folgendermaßen vor, um Tastenkombinationen festzulegen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Einstellungen**.
4. Wählen Sie im linken Fensterbereich den Abschnitt **Tastenkombinationen**.
5. Legen Sie im rechten Fensterbereich die für eine Aktion gewünschte Tastenkombination fest.

ORT DER KENNWORT-DATENBANK

Die Kennwort-Datenbank von Password Manager ist eine verschlüsselte Datei (s. S. 217), in der alle Ihre persönlichen Daten (Benutzerkonten, Benutzernamen, Kennwörter und Visitenkarten) gespeichert sind.

In den einzelnen Versionen von Microsoft Windows gelten folgende Standardpfade für die Kennwort-Datenbank:

- für Microsoft Windows XP: C:\Documents and Settings\User_name\My Documents\Passwords Database\
- für Microsoft Windows Vista: C:\Users\User_name\Documents\Passwords Database
- für Microsoft Windows 7: C:\Users\User_name\Documents\Passwords Database

Sie können als Speicher für Ihre Kennwort-Datenbank unterschiedliche Datenträger verwenden: Wechseldatenträger, lokaler Datenträger oder Netzlaufwerk.

Wenn der Pfad oder der Name der Kennwort-Datenbank geändert wird, bestehen folgende Varianten für das Vorgehen:

- **Kopieren** – Am angegebenen Pfad wird eine Kopie der Kennwort-Datenbank angelegt. Die Kopie wird zur aktiven Kennwort-Datenbank.
- **Verschieben** – Die aktive Kennwort-Datenbank wird am angegebenen Pfad gespeichert.

- **Neue Kennwort-Datenbank erstellen** – Es wird eine leere Kopie der Kennwort-Datenbank erstellt, die zur aktiven Datenbank wird.

Gehen Sie folgendermaßen vor, um eine Kennwort-Datenbank zu verschieben oder umzubenennen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Einstellungen**.
4. Wählen Sie im linken Bereich des Fensters den Abschnitt **Meine Kennwörter**.
5. Klicken Sie auf der rechten Fensterseite im Block **Pfad** auf die Schaltfläche , die sich auf der rechten Seite des Felds **Pfad** befindet.
6. Geben Sie im folgenden Fenster **Kennwort-Datenbank auswählen** den Pfad und den Namen der Datei an, und klicken Sie anschließend auf **Öffnen**.
7. Wählen Sie im folgenden Fenster **Ort der Kennwort-Datenbank** die gewünschte Aktion für die Kennwort-Datenbank.
8. Geben Sie im folgenden Fenster **Password Manager** das Master-Kennwort ein, um die Änderungen zu bestätigen.

Gehen Sie folgendermaßen vor, um die aktuelle Kennwort-Datenbank zu ändern:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Einstellungen**.
4. Wählen Sie im linken Bereich des Fensters den Abschnitt **Meine Kennwörter**.
5. Klicken Sie auf der rechten Fensterseite im Block **Pfad** auf die Schaltfläche , die sich auf der rechten Seite des Felds **Pfad** befindet.
6. Wählen Sie im folgenden Fenster **Kennwort-Datenbank auswählen** die Datei der Kennwort-Datenbank und klicken Sie auf **Öffnen**.
7. Geben Sie im folgenden Fenster **Password Manager** das Master-Kennwort ein, das für den Zugriff auf die ausgewählte Kennwort-Datenbank gilt.

NEUE KENNWORT-DATENBANK ANLEGEN

Password Manager erlaubt es, nacheinander mit mehreren Kennwort-Datenbanken zu arbeiten. Durch das Erstellen einer neuen Kennwort-Datenbank lassen sich Ihre persönlichen Daten aufteilen, indem sie in zwei oder mehr Kennwort-Datenbanken gespeichert werden. Bei Bedarf kann eine alte Kennwort-Datenbank wiederhergestellt werden. Password Manager schlägt vor, eine neue Kennwort-Datenbank zu erstellen, wenn die aktuelle Datenbank beschädigt wurde oder eine Wiederherstellung aus einer Sicherungskopie nicht möglich ist.

Gehen Sie folgendermaßen vor, um eine neue Kennwort-Datenbank zu erstellen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Einstellungen**.
4. Wählen Sie im linken Bereich des Fensters den Abschnitt **Meine Kennwörter**.

5. Klicken Sie auf der rechten Fensterseite im Block **Pfad** auf die Schaltfläche , die sich auf der rechten Seite des Felds **Pfad** befindet.

6. Geben Sie im folgenden Fenster **Kennwort-Datenbank auswählen** einen Speicherort und einen Namen für die Datei der Kennwort-Datenbank an, und klicken Sie dann auf **Öffnen**.

7. Wählen Sie im folgenden Fenster **Ort der Kennwort-Datenbank** die Aktion **Neue Kennwort-Datenbank erstellen** aus.

8. Geben Sie im Fenster **Neue Kennwort-Datenbank** im Block **Kennwort** ein Kennwort für den Zugriff auf die neue Datenbank an und wiederholen Sie es im Feld **Kennwort bestätigen**.

   Wenn die Wiederholung des Kennworts falsch ist, wird sie rot hervorgehoben.

   Wählen Sie im Block **Verschlüsselungsalgorithmus** einen Cryptographic Service Provider und die gewünschte Verschlüsselungsmethode (s. S.217).

9. Geben Sie im folgenden Fenster ein neues Master-Kennwort ein, um das Erstellen einer neuen Kennwort-Datenbank zu bestätigen.

SPEICHERORT FÜR EINE SICHERUNGSKOPIE

Bevor irgendwelche Änderungen Ihrer persönlichen Daten gespeichert werden, legt Password Manager automatisch Sicherungskopien der Kennwort-Datenbank an. Dadurch wird erlaubt, im Fall von Systemabbrüchen oder technischen Störungen einen Datenverlust zu vermeiden. Password Manager erstellt eine vollständige Kopie der Kennwort-Datenbank. Die Kopie entspricht dem Zustand vor dem Speichern der letzten Änderungen. Wenn eine Kennwort-Datenbank beschädigt wurde, können Sie die Daten aus der letzten Sicherungskopie der Kennwort-Datenbank wiederherstellen (s. S. 208).

Als Speicher für die Sicherungskopien der Kennwort-Datenbank kann ein Wechseldatenträger, lokaler Datenträger oder Netzlaufwerk.

Die Sicherungskopien werden abhängig vom Typ des Betriebssystems standardmäßig unter folgendem Pfad gespeichert:

- für Microsoft Windows XP: C:\Documents and Settings\User_name\My Documents\Passwords Database\
- für Microsoft Windows Vista: C:\Users\User_name\Documents\Passwords Database\
- für Microsoft Windows 7: C:\Users\User_name\My Documents\Passwords Database\

Gehen Sie folgendermaßen vor, um den Pfad für Sicherungskopien zu ändern:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.

3. Klicken Sie im folgenden Fenster **Einstellungen**.

4. Wählen Sie im linken Bereich des Fensters den Abschnitt **Meine Kennwörter**.

5. Klicken Sie auf der rechten Fensterseite im Block **Backup** auf die Schaltfläche , die sich auf der rechten Seite des Felds **Pfad** befindet.

6. Wählen Sie im folgenden Fenster **Ordner suchen** den Zielordner für die Sicherungskopien der Kennwort-Datenbank.

VERSCHLÜSSELUNGSMETHODE AUSWÄHLEN

Die Aufgabe der Kryptographie besteht im Schutz von Informationen vor unbefugtem Zugriff und unerlaubter Verbreitung. Die Hauptfunktion einer Chiffre besteht darin, eine verschlüsselte Nachricht über einen ungeschützten Kanal zu senden.

Für die Verschlüsselung und Entschlüsselung werden Schlüssel benötigt. Ein Schlüssel ist ein obligatorischer Parameter einer Chiffre. Erfolgen Verschlüsselung und Entschlüsselung mit dem gleichen Schlüssel, so handelt es sich um einen symmetrischen Algorithmus. Werden zwei Schlüssel eingesetzt, dann ist der Algorithmus asymmetrisch. Bei symmetrischen Chiffren wird zwischen Block- und Stromchiffrierung unterschieden. Eine beliebige Information wird (unabhängig vom Format der Ausgangsdaten) als binärer Code interpretiert. Bei der Blockverschlüsselung werden alle Daten in Blöcke unterteilt, die dann voneinander unabhängig verschlüsselt werden. Bei der Stromverschlüsselung werden Informationen bitweise chiffriert.

Password Manager bietet folgende symmetrische Verschlüsselungsalgorithmen:

- **DES**. Blockverschlüsselung mit einer standardmäßigen Schlüsselgröße von 56 Bit. Nach heutigen Maßstäben bietet DES kein hohes Schutzniveau. Der Algorithmus wird verwendet, wenn keine hohen Sicherheitsanforderungen gelten.

- **3DES**. Blockverschlüsselung, die auf DES beruht. Der größte Nachteil des vorhergehenden Algorithmus, die geringe Schlüsselgröße, wurde hier behoben. Die Schlüsselgröße ist für 3DES dreimal größer als für DES (56*3=168 Bit). Die Funktionsgeschwindigkeit ist dreimal geringer als bei DES, dafür ist die Sicherheit erheblich höher. 3DES wird häufiger verwendet, weil DES keine ausreichende Stabilität gegen die heutzutage verwendeten Technologien zum "Knacken" von Chiffren besitzt.

- **3DES TWO KEY**. Blockverschlüsselung, die auf DES beruht. Ein Algorithmus des Typs 3DES, für den die Schlüsselgröße 112 Bit beträgt (56*2).

- **RC2**. Blockverschlüsselung mit variabler Schlüssellänge mit relativ hoher Verarbeitungsgeschwindigkeit. Dieser Algorithmus ist schneller als DES. Im Hinblick auf Sicherheit und Stabilität gleicht er dem Algorithmus 3DES.

- **RC4**. Blockverschlüsselung mit variabler Schlüssellänge. Die Schlüsselgröße beträgt von 40 bis 256 Bit. Die Vorteile des Algorithmus liegen in der hohen Geschwindigkeit und der variablen Schlüsselgröße. Password Manager verwendet für die Datenverschlüsselung standardmäßig den Algorithmus RC4.

- **AES**. Symmetrischer Blockverschlüsselungsalgorithmus mit einer Schlüsselgröße von 128, 192 oder 256 Bit. Der Algorithmus garantiert ein hohes Sicherheitsniveau und genießt höchste Popularität.

Um im Betriebssystem Microsoft Windows Verschlüsselungsoperation auszuführen, wird ein Cryptographic Provider verwendet. Jeder Cryptographic Provider unterstützt mehrere Verschlüsselungsalgorithmus mit unterschiedlicher Schlüssellänge. Password Manager verwendet folgende in Microsoft Windows integrierte Cryptographic Provider:

- Microsoft Base Cryptographic Provider

- Microsoft Enhanced Cryptographic Provider

- Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype)

- Microsoft RSA/Schannel Cryptographic Provider

- Microsoft Strong Cryptographic Provider

Gehen Sie folgendermaßen vor, um den Verschlüsselungsalgorithmus zu ändern:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.

3. Klicken Sie im folgenden Fenster **Einstellungen**.

4. Wählen Sie im linken Bereich des Fensters den Abschnitt **Meine Kennwörter**.

5. Klicken Sie auf der rechten Fensterseite im Block Datenv**erschlüsselung** auf **Ändern**.

6. Geben Sie im folgenden Fenster **Verschlüsselungsalgorithmus** die Verschlüsselungseinstellungen an.

KENNWORT-DATENBANK AUTOMATISCH BLOCKIEREN

Nach dem Programmstart und nach Ablauf eines festgelegten Zeitraums, während dem der Computer inaktiv war, blockiert Password Manager die Kennwort-Datenbank automatisch. Sie können eine Zeitspanne festlegen, nach deren Ablauf die Kennwort-Datenbank blockiert werden soll. Der Wert des Intervalls kann zwischen 1 und 60 Minuten liegen. Es wird empfohlen, für das Blockieren der Kennwort-Datenbank einen Wert von 5-20 Minuten Inaktivität des Computers festzulegen. Sie können auch das automatische Blockieren der Kennwort-Datenbank deaktivieren.

Nach einer bestimmten Inaktivitätsdauer des Computers blockiert Password Manager die Kennwort-Datenbank automatisch. Wenn das automatische Blockieren des Computers deaktiviert wird, sind Ihre persönlichen Daten ungeschützt, wenn Sie sich vom Computer entfernen, ohne ihn zuvor manuell zu sperren.

Gehen Sie folgendermaßen vor, um den Zeitraum zu ändern, nach dem die Kennwort-Datenbank blockiert wird:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.

3. Klicken Sie im folgenden Fenster **Einstellungen**.

4. Wählen Sie im linken Bereich des Fensters den Abschnitt **Meine Kennwörter**.

5. Wählen Sie auf der rechten Fensterseite im Block **Automatisches Blockieren** aus der Dropdown-Liste eine Inaktivitätsdauer des Computers, nach deren Ablauf die Kennwort-Datenbank blockiert werden soll.

   Um das Blockieren der Kennwort-Datenbank zu deaktivieren, wählen Sie den Wert **Nie**.

AUTHENTIFIZIERUNGSMETHODE FÜR PASSWORD MANAGER ÄNDERN

Die Authentifizierung erlaubt es, den Zugriff auf Ihre persönlichen Daten zu kontrollieren. Die Authentifizierungsmethode wird beim ersten Start von Password Manager ausgewählt. Die Authentifizierungsmethode kann aber später geändert werden.

Gehen Sie folgendermaßen vor, um die Authentifizierungsmethode zu ändern:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.

3. Klicken Sie im folgenden Fenster **Einstellungen**.

4. Wählen Sie im linken Fensterbereich den Abschnitt **Authentifizierungsmethode**.

5. Wählen Sie auf der rechten Fensterseite im Block **Authentifizierungsmethode** in der Dropdown-Liste eine Authentifizierungsmethode.

SIEHE AUCH:

USB- oder Bluetooth-Geräte zur Authentifizierung verwenden 219

USB- ODER BLUETOOTH-GERÄTE ZUR AUTHENTIFIZIERUNG VERWENDEN

Für den Zugriff auf die Kennwort-Datenbank (s. S. 218) erlaubt Password Manager die Verwendung unterschiedlicher USB- und Bluetooth-Geräte.

Gehen Sie folgendermaßen vor, um für den Zugriff auf die Kennwort-Datenbank ein USB-Gerät zu verwenden:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf den Linkrogrammhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Einstellungen**.
4. Wählen Sie im linken Fensterbereich den Abschnitt **Authentifizierungsmethode**.
5. Wählen Sie auf der rechten Fensterseite im Block **Authentifizierungsmethode** in der Dropdown-Liste den Wert **USB-Gerät**.
6. Schließen Sie das tragbare Gerät an den Computer an.
7. Wählen Sie aus der Liste **Laufwerke** ein Gerät und klicken Sie auf **Installieren**. Neben dem ausgewählten Gerät erscheint das Symbol . Wenn das angeschlossene Gerät nicht auf der Liste steht, aktivieren Sie das Kontrollkästchen **Zusätzliche Geräte anzeigen**. Bei Bedarf können Sie das Authentifizierungsgerät durch Klick auf **Zurücksetzen** ändern.

Gehen Sie folgendermaßen vor, um für den Zugriff auf die Kennwort-Datenbank ein Bluetooth-Gerät zu verwenden:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Einstellungen**.
4. Wählen Sie im linken Fensterbereich den Abschnitt **Authentifizierungsmethode**.
5. Wählen Sie auf der rechten Fensterseite im Block **Authentifizierungsmethode** in der Dropdown-Liste den Wert **Bluetooth-Gerät**.
6. Aktivieren Sie die Bluetooth-Funktion zuerst auf Ihrem Computer und dann auf dem Gerät.
7. Wählen Sie ein Gerät aus der Liste **Telefone und Modems** und klicken Sie dann auf **Installieren**. Neben dem ausgewählten Gerät erscheint das Symbol . Bei Bedarf kann das Authentifizierungsgerät durch Klick auf **Zurücksetzen** geändert werden.

MASTER-KENNWORT ÄNDERN

Das Master-Kennwort wird beim ersten Start von Password Manager festgelegt. Es kann später geändert werden.

Bei einer Änderung des Master-Kennworts fordert Password Manager eine Bestätigung des eingegebenen Kennworts (wiederholte Eingabe des neuen Kennworts). Es ist nicht möglich, ein neues Kennwort ohne Bestätigung zu speichern. Wenn das eingegebene Kennwort und seine Wiederholung voneinander abweichen, wird die Wiederholung des Kennworts rot hervorgehoben. Beim Versuch das neue Kennwort zu speichern, erfolgt in diesem Fall ein Warnhinweis.

Gehen Sie folgendermaßen vor, um das Master-Kennwort zu ändern:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.

3. Klicken Sie im folgenden Fenster **Einstellungen**.
4. Wählen Sie im linken Fensterbereich den Abschnitt **Authentifizierungsmethode**.
5. Klicken Sie auf der rechten Fensterseite im Block **Kennwortschutz** auf **Ändern**.
6. Tragen Sie das neue Kennwort im folgenden Fenster **Kennwortschutz** in die Felder **Kennwort** und **Kennwort bestätigen** ein.

UNTERSTÜTZTE WEBBROWSER

Damit die Funktionen zur automatischen Aktivierung eines Benutzerkontos und die Titelleisten-Schaltflächen (s. S. 221) korrekt arbeiten, fordert Password Manager für bestimmte Webbrowser die Installation zusätzlicher Erweiterungen (Plug-ins). In der Grundeinstellung erfolgt die Installation von Erweiterungen beim ersten Start von Password Manager. Sie können zusätzlich ein erforderliches Plug-in installieren.

Der Password Manager bietet eine Liste der Webbrowser und Mailprogramme, in der jedes Programm den Status **Installiert** / **Nicht installiert** besitzt, je nachdem, ob ein entsprechendes Plug-in installiert wurde oder nicht.

Es wird empfohlen, alle Programme, für die Sie ein Plug-in installieren möchten, zu schließen.

Gehen Sie folgendermaßen vor, um ein Plug-in für einen Webbrowser oder ein Mailprogramm zu installieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Einstellungen**.
4. Wählen Sie im linken Fensterbereich den Abschnitt **Unterstützte Webbrowser**.
5. Wählen Sie auf der rechten Fensterseite aus der Liste **Unterstützte Webbrowser und verfügbare Erweiterungen** ein Programm und klicken Sie dann auf **Installieren**.
6. Folgen Sie den Hinweisen des **Installationsassistenten**. Nachdem ein Plug-in installiert wurde, wird der Name des Programms automatisch in die Gruppe **Installierte** Webbrowser verschoben. Es erhält den Status **Installiert**. Zum Löschen von installierten Erweiterungen dient die Schaltfläche **Löschen**.

VORLAGEN FÜR PERSÖNLICHE NOTIZEN VERWALTEN

Sie können die vorgegebenen Vorlagen für persönliche Notizen (s. S. 204) bearbeiten, neue Vorlagen erstellen oder eine vorhandene persönliche Notiz als Vorlage verwenden.

Gehen Sie folgendermaßen vor, um eine vorgegebene Vorlage für eine persönliche Notiz zu ändern:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Einstellungen**.
4. Wählen Sie auf der linken Fensterseite den Abschnitt **Vorlagen verwalten**.
5. Wählen Sie im rechten Fensterbereich eine Vorlage aus der Liste aus und klicken Sie auf **Ändern**.
6. Nehmen Sie im Texteditor die erforderlichen Änderungen vor.

Gehen Sie folgendermaßen vor, um eine Vorlage für eine persönliche Notiz zu erstellen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Einstellungen**.
4. Wählen Sie auf der linken Fensterseite den Abschnitt **Vorlagen verwalten**.
5. Klicken Sie auf der rechten Fensterseite auf **Hinzufügen**.
6. Geben Sie im folgenden Fenster im Feld **Name** einen Namen für die neue Notiz-Vorlage ein.
7. Geben Sie die entsprechenden Informationen im Texteditor ein.

Gehen Sie folgendermaßen vor, um eine vorhandene persönliche Notiz als Vorlage zu verwenden:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Password Manager** auf **Kennwort-Datenbank**.
4. Wählen Sie im folgenden Fenster die entsprechende Notiz aus der Liste ausund klicken Sie im oberen Fensterbereich auf **Ändern**.
5. Klicken Sie im folgenden Fenster unten auf **Als Vorlage speichern**.
6. Geben Sie im folgenden Fenster im Feld **Name** einen Namen für die neue Notiz-Vorlage ein.

TITELLEISTEN-SCHALTFLÄCHE ANZEIGEN

Wenn in ein Programm, mit dem Sie arbeiten, nicht nur das Menü von Password Manager, sondern auch Menüs anderer Programme integriert sind, können Sie die Position der Titelleisten-Schaltfläche im Verhältnis zu anderen Schaltflächen ändern, . Außerdem kann manuell eine Liste der Webbrowser angelegt werden, für die eine Titelleisten-Schaltfläche (s. S. 55) verwendet werden soll.

Gehen Sie folgendermaßen vor, um die Einstellungen für die Anzeige der Titelleisten-Schaltfläche zu ändern:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Einstellungen**.
4. Wählen Sie im linken Bereich des Fensters den Abschnitt **Titelleisten-Schaltfläche**.
5. Passen Sie auf der rechten Fensterseite im Block **Titelleisten-Schaltfläche anzeigen** die erforderlichen Parameter in Abhängigkeit von der Aufgabe an:
   - Um die Position der Titelleisten-Schaltfläche zu ändern, geben Sie im Feld **Schaltfläche nach links verschieben** eine Positionsnummer für die Schaltfläche ein (wie weit die Titelleisten-Schaltfläche nach links verschoben werden soll).
   - Damit die Titelleisten-Schaltfläche nicht angezeigt wird, wenn die Kennwort-Datenbank blockiert ist, aktivieren Sie das Kontrollkästchen **Nicht anzeigen wenn Password Manager blockiert wurde**.
   - Um eine Liste der Webbrowser anzulegen, in die die Titelleisten-Schaltfläche integriert werden soll, aktivieren Sie im Block **Titelleisten-Schaltfläche in folgenden Webbrowsern anzeigen** das Kontrollkästchen für die entsprechenden Webbrowser.

SPEICHERDAUER DES KENNWORTS IN DER ZWISCHENABLAGE

Password Manager erlaubt es, ein Kennwort für einen festgelegten Zeitraum in der Zwischenablage zu speichern. Diese Option ist nützlich, um schnell mit Kennwörtern zu arbeiten (beispielsweise wenn es erforderlich ist, ein erstelltes Kennwort bei der Anmeldung auf einer Webseite / in einem Programm zu verwenden). Sie können den Zeitraum festlegen, für den ein Kennwort in der Zwischenablage gespeichert werden soll. Nach Ablauf dieses Zeitraums wird das Kennwort automatisch aus der Zwischenablage gelöscht. Dies verhindert das Abfangen und den Diebstahl von Kennwörtern, weil ein Kennwort nach dem festgelegten Zeitraum nicht mehr aus der Zwischenablage kopiert werden kann.

Gehen Sie folgendermaßen vor, um festzulegen, wie lange ein Kennwort in der Zwischenablage gespeichert werden soll:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Einstellungen**.
4. Wählen Sie im linken Fensterbereich den Abschnitt **Allgemein**.
5. Legen Sie auf der Rechten Fensterseite im Block **Zwischenablage** eine Dauer in Sekunden fest.

MELDUNGEN

Bei der Arbeit von Password Manager treten unterschiedliche Arten von Ereignissen auf, die gewöhnlich informativen Charakter besitzen. Verwenden Sie den Benachrichtigungsdienst, um sich über Ereignisse informieren zu lassen. Der Benutzer wird durch Tooltipps und Popupmeldungen informiert.

Im Programm gibt es folgende Typen von Benachrichtigungen:

- **Programm starten**. Die Meldung erfolgt bei einem wiederholten Programmstart, wenn das Programm bereits gestartet und die Kennwort-Datenbank nicht blockiert wurde.
- **Benutzerkonto aktivieren**. Die Meldung erfolgt, wenn ein Benutzerkonto aktiviert wird.
- **Zwischenablage leeren**. Der Kenner-Manager erlaubt es, ein Kennwort vorübergehend in der Zwischenablage zu speichern. Dadurch lassen sich Daten bequem kopieren und in ein ausgewähltes Feld einfügen. Nach Ablauf einer festgelegten Zeitspanne (s. S. 222) wird das Kennwort aus der Zwischenablage gelöscht.
- **Password Manager automatisch blockieren**. Wenn Password Manager die Kennwort-Datenbank automatisch blockiert, erscheint eine Meldung. Die Kennwort-Datenbank wird nach dem Hochfahren des Betriebssystems und nach einem festgelegten Zeitraum (s. S. 218), während dem der Computer inaktiv war, automatisch blockiert.
- **Daten in eine ungeschützte Datei exportieren**. Warnmeldung, dass Ihre Kennwörter durch den Export in einer unverschlüsselten Datei gespeichert werden und dadurch jedem Benutzer, der auf Ihren Computer arbeitet, zugänglich sind. Es wird empfohlen, vor dem Export zu überlegen, wie die Datei mit den Kennwörtern geschützt werden kann.
- **Formular manuell ändern**. Um die Parameter von Zusatzfeldern anzupassen, fragt das Programm nach der Erlaubnis, den standardmäßig installierten Webbrowser zu verwenden. Die Meldung warnt davor, dass Bilder und Systemdateien (Cookies) auf Ihrem Computer gespeichert werden.
- **Probleme beim Ausfüllen eines Benutzernamens für ein Benutzerkonto**. Die Meldung warnt davor, dass es nicht möglich ist, bei der Authentifizierung automatisch Daten einzufügen.

Gehen Sie folgendermaßen vor, um Meldung erhalten:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Einstellungen**.
4. Wählen Sie im linken Fensterbereich den Abschnitt **Allgemein**.
5. Klicken Sie auf der rechten Fensterseite im Block **Allgemein** auf **Meldungseinstellungen**.
6. Aktivieren / deaktivieren Sie im folgenden Fenster das Kontrollkästchen für die entsprechenden Benachrichtigungstypen.

AKTION BEI DOPPELKLICK

Password Manager erlaubt es, eine Aktion festzulegen, die bei Doppelklick auf das Programmsymbol im Infobereich der Taskleiste von Microsoft Windows (s. S. 52) gestartet werden soll. Folgende Aktionen stehen zur Auswahl:

- Hauptfenster von Password Manager (s. S. 52) öffnen
- Password Manager blockieren/freigeben (Standardaktion)

Gehen Sie folgendermaßen vor, um die Aktion zu ändern, die durch Doppelklick auf das Programmsymbol im Infobereich der Taskleiste gestartet werden soll:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
3. Klicken Sie im folgenden Fenster **Einstellungen**.
4. Wählen Sie im linken Fensterbereich den Abschnitt **Allgemein**.
5. Wählen Sie auf der rechten Fensterseite in der Dropdown-Liste **Doppelklick auf das Symbol** eine Aktion.

ERSTELLEN VON SICHEREN KENNWÖRTERN

Die Datensicherheit ist direkt von der Stärke der Kennwörter abhängig. In folgenden Fällen können Daten einem Risiko unterliegen:

- Es wird für alle Benutzerkonten das gleiche Kennwort benutzt.
- einfaches Kennwort.
- Als Kennwort werden Informationen verwendet, die sich leicht erraten lassen (z.B. Namen von Familienmitgliedern oder ihre Geburtstage).

Um die Datensicherheit zu gewährleisten, besitzt Password Manager eine Funktion, mit der unter Verwendung eines Kennwort-Generators unikale und sichere Kennwörter für Benutzerkonten generiert werden können.

Ein Kennwort gilt als sicher, wenn es aus mehr als vier Zeichen besteht und Sonderzeichen, Ziffern, Groß- und Kleinbuchstaben darin verwendet werden.

Die Kennwortstärke wird durch folgende Parameter bestimmt:

- **Länge** – Anzahl der Zeichen in einem Kennwort. Der Wert kann zwischen 4 und 99 Zeichen liegen. Je länger ein Kennwort ist, desto sicherer ist es.
- **A-Z** – Verwendung von Großbuchstaben.
- **a-z** – Verwendung von Kleinbuchstaben.

- **0-9** – Verwendung von Ziffern.
- **Sonderzeichen** – Verwendung von Sonderzeichen.
- **Zeichen nicht doppelt verwenden** – Verbot der Verwendung von gleichen Zeichen in einem Kennwort.

Gehen Sie folgendermaßen vor, um mit dem Kennwort-Generator ein sicheres Kennwort zu erstellen:

1. Öffnen Sie das Kontextmenü des Kennwort-Managers und wählen Sie den Punkt **Kennwort-Generator**.
2. Geben Sie im folgenden Fenster **Kennwort-Generator** im Feld **Länge des Kennworts** die Anzahl der Zeichen im Kennwort an.
3. Passen Sie bei Bedarf zusätzliche Parameter für den Kennwort-Generator an. Aktivieren / deaktivieren Sie dazu im Block **Erweiterte Einstellungen** das Kontrollkästchen der entsprechenden Parameter.
4. Klicken Sie auf **Generieren**. Das erstellte Kennwort wird im Feld **Kennwort** angezeigt. Um das generierte Kennwort zu lesen, aktivieren Sie das Kontrollkästchen **Kennwort anzeigen**.
5. Kopieren Sie das Kennwort mit der Schaltfläche in die Zwischenablage und fügen Sie es dann mit der Tastenkombination **STRG+V** in einem Programm / auf einer Webseite ein. Das erstellte Kennwort wird in der Zwischenablage gespeichert.
6. Aktivieren Sie das Kontrollkästchen **Standard**, um die ausgewählten Einstellungen zur späteren Verwendung zu speichern.

VERWENDUNG EINER PORTABLEN VERSION DES PASSWORD MANAGERS

Password Manager erlaubt es, alle Kennwörter auf einem Wechseldatenträger zu speichern (z.B. auf einer Speicherkarte oder auf einem Mobiltelefon, wenn dieses als Speicherkarte verwendet wird). Dazu ist es erforderlich, auf einem Wechseldatenträger eine portable Version des Password Managers zu erstellen. Die portable Programmversion wird auf dem Computer erstellt, auf dem die Vollversion von Password Manager installiert ist. Die portable Programmversion besitzt die vollständige Funktionalität von Password Manager.

Die portable Version erlaubt es, den Password Manager auf einem allgemein zugänglichen Computer zu verwenden (z.B. im Internet-Café oder in einer Bibliothek), auf dem Password Manager nicht installiert ist. Wenn der Wechseldatenträger mit dem Computer verbunden wird, startet Password Manager automatisch. Beim Trennen des Wechseldatenträgers wird Password Manager automatisch geschlossen und auf dem öffentlichen Computer verbleiben keine Spuren Ihrer Daten.

Außerdem können Sie mit Hilfe der portablen Version Ihre Kennwort-Datenbanken synchronisieren, wenn Password Manager installiert ist und parallel auf verschiedenen Computern verwendet wird (z.B. zuhause und im Büro).

IN DIESEM ABSCHNITT

Portable Version erstellen und verbinden..... 224

Synchronisierung der Kennwort-Datenbank..... 225

PORTABLE VERSION ERSTELLEN UND VERBINDEN

Um zu gewährleisten, dass die portable Version des Password Managers auf einem öffentlich zugänglichen Computer richtig funktioniert, wird empfohlen, die zusätzlichen Plug-ins für den Webbrowser zu installieren.

Ein Plug-in kann auf eine der folgenden Arten installiert werden:

- Aus dem Fenster des Assistenten zur Plug-in-Installation. Folgen Sie dazu beim ersten Start der portablen Version von Password Manager den Anweisungen des Assistenten zur Plug-in-Installation.

- Aus dem Menü der Titelleisten-Schaltfläche im Fenster des Webbrowsers. Wählen Sie dazu im Menü der Titelleisten-Schaltfläche den Punkt **Autoausfüllen-Plug-in nicht installiert** aus.

Beim ersten Start auf einem öffentlichen Computer wird automatisch der Installationsassistent für die portable Version von Password Manager gestartet. Ihnen wird angeboten, folgende Zusatzparameter für die Verwendung der portablen Programmversion festzulegen:

- Verknüpfung auf Desktop erstellen - Mit dieser Verknüpfung kann das Programm künftig vom Desktop des Computers aus gestartet werden.

- Virtuelle Tastatur verwenden – Öffnet die virtuelle Tastatur zur Eingabe von persönlichen Daten.

Gehen Sie folgendermaßen vor, um eine portable Version des Password Managers zu erstellen:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im unteren Fensterbereich auf **Password Manager**.

3. Klicken Sie im folgenden Fenster auf **Portable Version**.

4. Wählen Sie im folgenden Fenster das Gerät aus, auf das Sie die portable Version von Password Manager installieren wollen, und klicken Sie auf **Weiter**.

5. Legen Sie im folgenden Fenster die Einstellungen für die portable Version fest:

   - Um das Master-Kennwort für den Zugriff auf die portable Version von Password Manager nicht einzugeben, aktivieren Sie das Kontrollkästchen **Nie nach Master-Kennwort fragen**.

   - Damit die portable Version automatisch gestartet wird, wenn der Wechseldatenträger mit einem Computer verbunden wird, aktivieren Sie das Kontrollkästchen **Autostart von Password Manager von einem portablen Gerät aktivieren**.

6. Klicken Sie auf **Ausführen**. Klicken Sie nach dem Abschluss der Installation auf **Fertig**.

Gehen Sie folgendermaßen vor, um die portable Programmversion zu verwenden:

1. Schließen Sie den Wechseldatenträger an den Computer an.

2. Starten Sie die portable Version von Password Manager von dem ausgewählten Wechseldatenträger, falls diese beim Anschließen des Datenträgers nicht automatisch gestartet wurde.

3. Beim ersten Start der portablen Version wird Ihnen vorgeschlagen, die Autoausfüllen-Plug-ins zu installieren und die Kennwort-Manager zu deaktivieren, die in den auf Ihrem Computer installierten Webbrowsern integriert sind.

4. Geben Sie im folgenden Fenster das Master-Kennwort ein.

   Die portable Version des Password Managers ist zur Verwendung bereit.

SYNCHRONISIERUNG DER KENNWORT-DATENBANK

Wenn Sie den Password Manager auf unterschiedlichen Computern einsetzen, ist es erforderlich, alle Kennwort-Datenbanken aktuell zu halten. Mit der portablen Programmversion können Sie die Daten synchronisieren und auf allen Computern, auf denen der Password Manager installiert ist, die aktuelle Kennwort-Datenbank verwenden. Synchronisieren Sie dazu die Kennwort-Datenbank der portablen Version mit der Kennwort-Datenbank auf einem der Computer und wiederholen Sie die Synchronisierung dann auf einem anderen Computer.

Gehen Sie folgendermaßen vor, um die Kennwort-Datenbank der portablen Version mit der Kennwort-Datenbank auf einem der Computer zu synchronisieren:

1. Schließen Sie den Wechseldatenträger an den Computer an.
2. Öffnen Sie das Programmhauptfenster.
3. Klicken Sie im unteren Fensterbereich auf **Password Manager**.
4. Klicken Sie im folgenden Fenster auf **Portable Version**.
5. Wählen Sie im folgenden Fenster das Gerät aus, auf dem die portable Version des Password Managers installiert ist, und klicken Sie auf **Weiter**.
6. Wählen Sie im folgenden Fenster eine Synchronisierungsmethode für die Kennwort-Datenbank aus:
   - Um die Daten aus der Datenbank des Password Managers, der auf dem Computer installiert ist, zur Kennwort-Datenbank der portablen Version hinzuzufügen, wählen Sie die Variante **Kennwort-Datenbanken zusammenführen** aus

     Die Datenbank des Password Managers auf dem Computer bleibt dabei unverändert. Um die zusammengeführten Daten in diese Datenbank aufzunehmen, wiederholen Sie die Synchronisierung und wählen Sie die Variante **Kennwort-Datenbank der portablen Version verwenden**.
   - Um die Kennwort-Datenbank der portablen Version durch die Datenbank des auf dem Computer installierten Password Managers zu ersetzen, wählen Sie in der portablen Version die Variante **Datenbank des auf dem Computer installierten Password Managers verwenden** aus.
   - Um die Datenbank des auf dem Computer installierten Password Managers durch die Kennwort-Datenbank der portablen Version zu ersetzen, wählen Sie die Variante **Kennwort-Datenbank der portablen Version verwenden** aus.
7. Klicken Sie auf **Weiter**.
8. Legen Sie im folgenden Fenster die Einstellungen für die portable Version fest:
   - Um das Master-Kennwort für den Zugriff auf die portable Version von Password Manager nicht einzugeben, aktivieren Sie das Kontrollkästchen **Nie nach Master-Kennwort fragen**.
   - Damit die portable Version automatisch gestartet wird, wenn der Wechseldatenträger mit einem Computer verbunden wird, aktivieren Sie das Kontrollkästchen **Autostart von Password Manager von einem portablen Gerät aktivieren**.
9. Klicken Sie auf **Ausführen**. Klicken Sie nach dem Abschluss der Synchronisierung auf **Fertig**.

LEISTUNG UND KOMPATIBILITÄT MIT ANDEREN PROGRAMMEN

Die Leistungseinstellungen für Kaspersky PURE umfassen das Spektrum der erkennbaren Bedrohungen sowie Energieverbrauch und benötigte Computerressourcen.

Kaspersky PURE erlaubt es, das Schutzspektrum flexibel anzupassen und unterschiedliche Bedrohungskategorien (s. Abschnitt "Kategorien der erkennbaren Bedrohungen wählen" auf S. 227) zu wählen, die das Programm bei der Arbeit erkennen soll.

Bei der Arbeit auf einem Laptop besitzt der Energieverbrauch, der von Programmen verursacht wird, eine besondere Bedeutung. Eine Virenuntersuchung des Computers und das Datenbank-Update beanspruchen erhebliche Ressourcen. Ein spezieller Modus für die Arbeit von Kaspersky PURE auf einem Laptop (s. S. 229) schiebt geplante Untersuchungs-

und Updateaufgaben automatisch auf, wenn die Stromversorgung von einer Batterie erfolgt, und spart dadurch Akkustrom.

Der von Kaspersky PURE verursachte Verbrauch von Computerressourcen kann sich auf die Performance anderer Programme auswirken. Um bei der gleichzeitigen Arbeit mit anderen Programmen Probleme durch eine hohe Last auf Prozessor und Laufwerk-Subsysteme zu vermeiden, kann Kaspersky PURE Untersuchungsaufgaben anhalten und Ressourcen für andere Programme freigeben (s. S. 228), die auf dem Computer laufen.

Im Modus Profil für Spiele wird die Anzeige von Meldungen über die Arbeit von Kaspersky PURE automatisch deaktiviert, wenn andere Programme im Vollbildmodus gestartet werden.

Der erweiterte Desinfektionsvorgang, der für den Fall einer aktiven Infektion vorgesehen ist, erfordert einen obligatorischen Neustart des Computers, was sich ebenfalls auf die Arbeit anderer Programme auswirken kann. Bei Bedarf können Sie die Verwendung der Technologie zur Desinfektion aktiver Infektionen (s. S. 227) deaktivieren, um eine unerwünscht hohe Auslastung des Computers zu vermeiden.

IN DIESEM ABSCHNITT

Kategorien der erkennbaren Bedrohungen auswählen 227

Technologie zur Desinfektion einer aktiven Infektion 227

Verteilung der Computerressourcen bei der Virensuche 228

Programmparameter bei der Arbeit im Vollbildmodus. Profil für Spiele 228

Energiesparen im Akkubetrieb 229

KATEGORIEN DER ERKENNBAREN BEDROHUNGEN AUSWÄHLEN

Die Bedrohungen, die von Kaspersky PURE erkannt werden, sind nach unterschiedlichen Merkmalen in Kategorien angeordnet. Viren, trojanische Programme und schädliche Tools werden immer vom Programm erkannt. Diese Programme können Ihrem Computer bedeutenden Schaden zufügen. Zur Steigerung der Computersicherheit lässt sich die Liste der zu erkennenden Bedrohungen durch Aktivierung der Kontrolle des Verhaltens legaler Programme erweitern, die von Angreifern zur Schädigung des Computers oder der Daten des Benutzers verwendet werden können.

Gehen Sie folgendermaßen vor, um die Kategorien erkennbare Bedrohungen auszuwählen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** den Abschnitt **Bedrohungen und Ausnahmen**.
4. Klicken Sie auf der rechten Fensterseite im Block **Bedrohungen** auf **Einstellungen**.
5. Aktivieren Sie im folgenden Fenster **Bedrohungen** die Kontrollkästchen für die Bedrohungen, die erkannt werden sollen.

TECHNOLOGIE ZUR DESINFEKTION EINER AKTIVEN INFEKTION

Moderne Schadprogramme können in die tiefste Ebene des Betriebssystems eindringen, wodurch es praktisch unmöglich wird, sie zu löschen. Wenn Kaspersky PURE eine schädliche Aktivität im System erkennt, bietet er an, einen speziell dafür vorgesehenen erweiterten Desinfektionsvorgang auszuführen, durch den die Bedrohung neutralisiert und vom Computer gelöscht wird.

Zum Abschluss des Vorgangs erfolgt ein obligatorischer Neustart des Computers. Nach dem Neustart des Computers wird empfohlen, eine vollständige Virenuntersuchung zu starten (s. Abschnitt "Wie eine vollständige Virenuntersuchung des Computers ausgeführt wird" auf S. 68).

- *Gehen Sie folgendermaßen vor, damit Kaspersky PURE die Prozedur zur erweiterten Desinfektion anwendet:*

  1. Öffnen Sie das Programmhauptfenster.
  2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
  3. Wählen Sie auf der linken Fensterseite im Abschnitt **Allgemeine Einstellungen** den Abschnitt **Kompatibilität**.
  4. Aktivieren Sie im rechten Fensterbereich das Kontrollkästchen **Technologie zur aktiven Desinfektion verwenden**.

VERTEILUNG DER COMPUTERRESSOURCEN BEI DER VIRENSUCHE

Um die Belastung des Prozessors und der Laufwerkssubsysteme zu reduzieren, können Sie festlegen, dass Aufgaben zur Virensuche aufgeschoben werden.

Das Ausführen von Untersuchungsaufgaben erhöht die Auslastung des Prozessors und der Laufwerkssubsysteme und verlangsamt dadurch die Arbeit anderer Programme. In der Grundeinstellung hält Kaspersky PURE beim Eintreten dieser Situation die Ausführung von Untersuchungsaufgaben an und gibt Systemressourcen für Benutzeranwendungen frei.

Allerdings existiert eine Reihe von Programmen, die gestartet werden, wenn Prozessorressourcen frei werden, und im Hintergrundmodus arbeiten. Wenn die Untersuchung von der Arbeit solcher Programme unabhängig sein soll, sollten ihnen keine Systemressourcen überlassen werden.

Beachten Sie, dass dieser Parameter für jede Untersuchungsaufgabe individuell angepasst werden kann. In diesem Fall besitzt der für eine konkrete Aufgabe festgelegte Parameter die höchste Priorität.

- *Gehen Sie folgendermaßen vor, damit Kaspersky PURE die Untersuchungsaufgaben zurückstellt, wenn sie die Arbeit anderer Programme verlangsamen:*

  1. Öffnen Sie das Programmhauptfenster.
  2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
  3. Wählen Sie auf der linken Fensterseite im Abschnitt **Allgemeine Einstellungen** den Abschnitt **Kompatibilität**.
  4. Aktivieren Sie im rechten Fensterbereich das Kontrollkästchen **Ressourcen für andere Programme freigeben**.

PROGRAMMPARAMETER BEI DER ARBEIT IM VOLLBILDMODUS. PROFIL FÜR SPIELE

Die Verwendung bestimmter Programme (insbesondere von Computerspielen) im Vollbildmodus ist für die Kompatibilität mit einigen Funktionen von Kaspersky PURE problematisch. In diesem Modus sind beispielsweise Meldungsfenster unangebracht. Teilweise nehmen solche Programme auch erhebliche Systemressourcen in Anspruch, sodass die Ausführung einer Aufgabe von Kaspersky PURE zur einer Verlangsamung dieser Programme führen kann.

Damit der Benutzer nicht jedes Mal, wenn er in den Vollbildmodus wechselt, manuell die Benachrichtigungen deaktivieren und Aufgaben anhalten muss, bietet Kaspersky PURE die Möglichkeit, diese Parameter mit Hilfe eines Profils für Spiele vorübergehend zu ändern. Wenn das Spiele-Profils aktiviert wird, werden beim Wechsel in den Vollbildmodus automatisch die Parameter aller Komponenten so geändert, dass eine optimale Arbeit in diesem Modus gewährleistet ist. Bei Verlassen des Vollbildmodus werden für die Parameter des Programms die Werte wiederhergestellt, die vor dem Wechsel in den Vollbildmodus eingestellt waren.

Gehen Sie folgendermaßen vor, um die Verwendung des Profils für Spiele zu aktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Allgemeine Einstellungen** den Abschnitt **Profil für Spiele**.
4. Aktivieren Sie das Kontrollkästchen **Profil für Spiele verwenden** und geben Sie darunter im Block **Einstellungen für Profil** die erforderlichen Parameter für die Verwendung des Spiele-Profils an.

ENERGIESPAREN IM AKKUBETRIEB

Um sparsam mit der Batterie eines Laptops umzugehen, können Sie Aufgaben zur Virensuche und zum Update nach Zeitplan aufschieben. Bei Bedarf können Sie Kaspersky PURE auf Befehl aktualisieren oder die Virenuntersuchung manuell starten.

Gehen Sie folgendermaßen vor, um den Energiesparmodus bei Akkubetrieb zu aktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Allgemeine Einstellungen** den Abschnitt **Energiesparen**.
4. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Geplante Untersuchungsaufgaben bei Akkubetrieb nicht starten**.

SELBSTSCHUTZ FÜR KASPERSKY PURE

Da Kaspersky PURE für die Sicherheit des Computers vor schädlichen Programmen verantwortlich ist, versuchen bestimmte Schadprogramme, die auf den Computer gelangen, die Arbeit von Kaspersky Internet Security zu blockieren oder ihn sogar vom Computer zu löschen.

Die Stabilität des Sicherheitssystems für Ihren Computer wird in Kaspersky PURE durch Mechanismen zum Selbstschutz und zum Schutz vor externem Zugriff realisiert.

Der Selbstschutz für Kaspersky PURE verhindert, dass seine Dateien auf der Festplatte, Prozesse im Speicher und Einträge in der Registrierung verändert oder gelöscht werden. Der Schutz vor externem Zugriff kann alle Versuche zur Fernsteuerung der Programmdienste blockieren.

Für 64-Bit-Betriebssysteme und für Microsoft Windows Vista steht der Selbstschutzmechanismus von Kaspersky PURE nur im Hinblick auf Veränderungen oder Löschen von eigenen Dateien auf der Festplatte und Veränderungen oder Löschen von Einträgen in der Systemregistrierung zur Verfügung.

IN DIESEM ABSCHNITT

Selbstschutz aktivieren und deaktivieren 230

Schutz vor externer Steuerung..... 230

SELBSTSCHUTZ AKTIVIEREN UND DEAKTIVIEREN

Der Selbstschutz von Kaspersky PURE ist standardmäßig aktiviert. Bei Bedarf können Sie den Selbstschutz deaktivieren.

Gehen Sie folgendermaßen vor, um den Selbstschutz von Kaspersky PURE zu aktivieren oder zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Allgemeine Einstellungen** den Abschnitt **Selbstschutz**.
4. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Selbstschutz aktivieren**, um den Selbstschutz von Kaspersky PURE auszuschalten. Aktivieren Sie dieses Kontrollkästchen, um den Selbstschutz einzuschalten.

SCHUTZ VOR EXTERNER STEUERUNG

Der Schutz vor externer Steuerung ist standardmäßig aktiviert. Bei Bedarf können Sie den Schutz deaktivieren.

Wenn der Schutz vor Fernsteuerung aktiviert ist, kann es vorkommen, dass gleichzeitig Programme, die der Remote-Administration dienen, eingesetzt werden sollen (z.B. RemoteAdmin). Um die Arbeit dieser Programme zu ermöglichen, werden sie zur Liste der vertrauenswürdigen Programme (s. Abschnitt "Liste mit vertrauenswürdigen Programmen erstellen" auf S. 162) hinzugefügt, und die Einstellung **Programmaktivität nicht kontrollieren** wird für sie aktiviert.

Gehen Sie folgendermaßen vor, um den Schutz vor externer Steuerung zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Allgemeine Einstellungen** den Abschnitt **Selbstschutz**.
4. Deaktivieren Sie im rechten Fensterbereich im Block **Externe Steuerung** das Kontrollkästchen **Option zur externen Steuerung des Systemdienstes deaktivieren**.

AUSSEHEN DES PROGRAMMS

Sie können das Aussehen von Kaspersky PURE verändern, indem Sie alternative grafische Oberflächen verwenden. Zusätzlich besteht die Möglichkeit, aktive Elemente der Benutzeroberfläche anzupassen (Programmsymbol im Infobereich der Microsoft Windows-Taskleiste und Popupmeldungen).

IN DIESEM ABSCHNITT

Aktive Elemente der Benutzeroberfläche 231

Grafische Oberfläche von Kaspersky PURE 231

News Agent 231

AKTIVE ELEMENTE DER BENUTZEROBERFLÄCHE

Sie können die Anzeige von aktiven Elementen der Benutzeroberfläche anpassen: z.B. Meldungsfenster, Symbol von Kaspersky PURE im Infobereich der Taskleiste.

Gehen Sie folgendermaßen vor, um die aktiven Elemente der Benutzeroberfläche anzupassen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Allgemeine Einstellungen** den Abschnitt **Ansicht**.
4. Aktivieren oder deaktivieren Sie im rechten Fensterbereich im Block **Symbol in der Taskleiste** die entsprechenden Kontrollkästchen.

GRAFISCHE OBERFLÄCHE VON KASPERSKY PURE

Alle auf der Oberfläche von Kaspersky PURE verwendeten Farben, Schriften, Piktogramme und Texte können verändert werden. Sie können eine individuelle grafische Oberfläche für das Programm erstellen und es in einer anderen Sprache lokalisieren.

Gehen Sie folgendermaßen vor, um eine andere grafische Oberfläche zu verwenden:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Allgemeine Einstellungen** den Abschnitt **Ansicht**.
4. Aktivieren Sie auf der rechten Fensterseite Grafische Oberflächen das Kontrollkästchen **Alternative Programmoberfläche verwenden**, um eine grafische Oberfläche einzubinden. Geben Sie im Eingabefeld den Ordner mit den Einstellungen der grafischen Oberfläche an oder klicken Sie auf **Durchsuchen**, um diesen Ordner zu suchen.

NEWS AGENT

Mit Hilfe von *News Agent* werden Sie von Kaspersky Lab über alle wichtigen Ereignisse informiert, die mit Kaspersky PURE und generell mit dem Schutz vor Computerbedrohungen zusammenhängen.

Wenn neue Nachrichten eintreffen, werden Sie vom Programm durch eine Popupmeldung im Infobereich der Taskleiste benachrichtigt. In diesem Fall verändert sich das Aussehen des Symbols (s. unten).

Die Nachrichten können folgendermaßen gelesen werden:

- Klicken Sie im Infobereich der Taskleiste auf das Symbol .
- Klicken Sie in der News-Popupmeldung auf den Link **Nachrichten lesen**.

Gehen Sie folgendermaßen vor, um den Nachrichten-Empfang zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie auf der linken Fensterseite im Abschnitt **Allgemeine Einstellungen** den Abschnitt **Ansicht**.

4. Deaktivieren Sie im rechten Fensterbereich im Block **Symbol in der Taskleiste** das Kontrollkästchen **Über Neuigkeiten benachrichtigen**.

ZUSÄTZLICHE FUNKTIONEN

Zum Lieferumfang von Kaspersky PURE gehören verschiedene Assistenten und Tools, mit denen Aufgaben für die Computersicherheit gelöst werden.

- Der Assistent zum Erstellen einer Notfall-CD dient dazu, eine Notfall-CD zu erstellen, mit der sich die Funktionsfähigkeit des Systems nach einem Virenangriff durch Booten von einem Wechseldatenträger wiederherstellen lässt. Die Notfall-CD kommt dann zum Einsatz, wenn der Infektionsgrad so hoch ist, dass die Desinfektion eines Computers nicht mehr mit Hilfe von Antiviren-Anwendungen oder Desinfektionstools möglich ist.

- Der Assistent zum Löschen von Aktivitätsspuren dient dazu, im System nach Aktivitätsspuren eines Benutzers sowie auch nach Betriebssystemparametern, die zum Sammeln von Informationen über die Aktivität des Benutzers dienen, zu suchen und diese zu beseitigen.

- Der Assistent zum Löschen von nicht mehr benötigten Informationen sucht und löscht temporäre und nicht mehr benötigte Dateien auf Ihrem Computer und optimiert die Arbeit des Systems.

- Der Assistent zur Systemwiederherstellung dient dazu, Beschädigungen des Systems und die Spuren von schädlichen Objekten im System zu beseitigen.

- Der Assistent zur Browser-Konfiguration dient dazu, die Parameter des Browsers Microsoft Internet Explorer zu analysieren und anzupassen, um potentielle Schwachstellen zu beseitigen.

- Die Funktion zum unwiderruflichen Löschen von Daten löscht vertrauliche Daten unwiderruflich, damit sie später nicht wiederhergestellt werden können.

Alle Probleme, die von den Assistenten gefunden werden (unter Ausnahme des Assistenten zum Erstellen einer Notfall-CD) werden im Hinblick auf die von ihnen für das System ausgehende Gefahr eingeteilt. Für jede Gruppe von Problemen schlagen die Kaspersky-Lab-Spezialisten eine Auswahl von Aktionen vor, mit denen die Schwachstellen und kritischen Punkte im System behoben werden können. Die Probleme und die entsprechenden Aktionen werden in drei Gruppen unterteilt:

- *Ausdrücklich empfohlene Aktionen* können Probleme beheben, die eine ernsthafte Sicherheitsbedrohung darstellen. Es wird empfohlen, alle Aktionen dieser Gruppe rechtzeitig auszuführen, um die Bedrohungen zu beseitigen.

- *Empfohlene Aktionen* dienen zum Beheben von Problemen, die ein potentielles Risiko darstellen können. Um einen optimalen Schutz zu gewährleisten, sollten auch die Aktionen dieser Gruppe ausgeführt werden.

- *Zusätzliche Aktionen* dienen dazu, momentan ungefährliche Probleme zu beheben, die die Computersicherheit aber in Zukunft bedrohen können. Diese Vorgehensweise sorgt für einen vollständigen Schutz Ihres Computers, kann aber in einigen Fällen zu einem Löschen von Benutzerparametern (z.B. von Cookies) führen.

IN DIESEM ABSCHNITT

Unwiderrufliches Löschen von Daten 234

Aktivitätsspuren löschen 235

Nicht verwendete Informationen löschen 236

Browser-Konfiguration 238

UNWIDERRUFLICHES LÖSCHEN VON DATEN

Die Datensicherheit umfasst nicht nur den Schutz vor Viren, Trojanern und sonstiger Malware, sondern auch den Schutz vor unerlaubter Wiederherstellung gelöschter Informationen.

Wenn Daten mit den standardmäßigen Methoden von Microsoft Windows gelöscht werden, gibt es keinen ausreichenden Schutz gegen eine mögliche Wiederherstellung. Gelöschte Daten verschwinden nicht von der Festplatte, sondern es werden nur die entsprechenden Laufwerkssektoren als frei markiert. Es wird lediglich der Eintrag über eine Datei in der Dateientabelle entfernt. Auch eine Formatierung von Datenträgern (z.B. Festplatte, Speicherkarte oder USB-Stick) garantiert nicht das unwiderrufliche Löschen von Daten. Man geht davon aus, dass Daten erst dann für immer verschwinden, wenn sie mehrmals überschrieben wurden. Doch selbst in diesem Fall können Informationen mit Hilfe leistungsfähiger Programme rekonstruiert werden.

Kaspersky PURE verfügt über einen Assistenten zum unwiderruflichen Löschen von Daten. Dieser Assistent erlaubt es, sensible Daten so zu löschen, dass sie nicht von Angreifern wiederhergestellt und verwendet werden können. Die unwiderrufliche Datenlöschung schließt die Möglichkeit aus, gelöschte Informationen mit herkömmlichen Programmen wiederherzustellen. Der Assistent kann für kleine und umfangreiche Objekte (bis zu mehreren Gigabyte) verwendet werden.

Der Assistent unterstützt die Datenlöschung von folgenden Datenträgern:

- Lokale Datenträger. Das Löschen ist möglich, wenn der Benutzer zum Schreiben und Löschen von Informationen berechtigt ist.

- Wechseldatenträger oder andere Geräte, die als Wechseldatenträger erkannt werden (z.B. Disketten, Flash Cards, USB-Sticks oder Mobiltelefone). Das Löschen von Speicherkarten ist möglich, wenn kein mechanischer Schreibschutz (Lock-Modus) besteht.

Vor dem unwiderruflichen Löschen prüft das Programm, ob die Datenlöschung von dem ausgewählten Datenträger möglich ist. Der Löschvorgang erfolgt nur, wenn die Datenlöschung auf dem ausgewählten Datenträger unterstützt wird. Andernfalls ist das unwiderrufliche Löschen von Daten nicht möglich.

Sie können nur Daten löschen, für die Ihr Benutzerkonto eine Zugriffsberechtigung besitzt. Vergewissern Sie sich vor der Löschung, dass die Datei oder der Ordner nicht geöffnet ist oder von anderen Programmen verwendet wird.

Es können Objekte wie eine Datei oder ein Ordner gelöscht werden. Um ein versehentliches Löschen wichtiger Daten zu verhindern, kann jeweils nur eine Datei oder ein Ordner zum Löschen ausgewählt werden (Ein zum Löschen ausgewählter Ordner kann dabei mehrere Dateien oder Unterordner enthalten).

Ein Ordner, der zum Löschen ausgewählt wurde, kann Systemdateien enthalten, deren Fehlen zu Systemstörungen führen könnte. Wenn sich unter den ausgewählten Daten Systemdateien oder -ordner befinden, erfolgt eine zusätzliche Abfrage zur Löschbestätigung.

Die Methoden zur unwiderruflichen Löschung persönlicher Daten sind standardisiert. Sie beruhen alle auf dem mehrfachen Überschreiben der zu löschenden Informationen durch Nullen, Einsen oder zufällige Zeichen. Geschwindigkeit und Qualität der Löschung sind von der Zyklenanzahl abhängig.

Gehen Sie folgendermaßen vor, um Daten unwiderruflich zu löschen:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im unteren Fensterbereich auf **Zusätzliche Funktionen**.

3. Klicken Sie im folgenden Fenster auf **Unwiderrufliches Löschen von Daten**.

4. Wählen Sie im folgenden Fenster **Unwiderrufliches Löschen von Daten** ein Objekt. Klicken Sie dazu auf **Durchsuchen** und wählen Sie im folgenden Fenster **Ordner auswählen** ein zu löschendes Objekt.

   Werden Sie in der Dropdown-Liste **Methode zum Löschen von Daten** einen Algorithmus zur Datenlöschung aus.

5. Bestätigen Sie das Löschen von Daten im folgenden Fenster durch Klick auf **OK**. Wenn bestimmte Dateien nicht gelöscht wurden, wiederholen Sie die Löschung durch Klick auf **Wiederholen**. Klicken Sie auf **Beenden**, um ein anderes Objekt zum Löschen auszuwählen.

AKTIVITÄTSSPUREN LÖSCHEN

Während der Arbeit auf dem Computer werden die Aktionen des Benutzers im System registriert. Dabei werden Daten darüber gespeichert, welche Suchanfragen der Benutzer vornimmt, welche Seiten er besucht, welche Programme er startet und welche Dateien er öffnet und speichert. Außerdem werden Einträge im Systemjournal von Microsoft Windows, temporäre Dateien u.v.a gespeichert.

Alle genannten Informationsquellen über die Benutzeraktivität können sensible Daten (darunter auch Kennwörter) enthalten und können unter Umständen von Angreifern entwendet und analysiert werden. Viele Benutzer verfügen nicht über ausreichende Kenntnisse, um einem Diebstahl wertvoller Informationen aus solchen Quellen vorzubeugen.

Kaspersky PURE verfügt über einen Assistenten zum Löschen von Aktivitätsspuren. Dieser Assistent führt im System die Suche nach Spuren von Benutzeraktivität und den Betriebssystemsparametern, die zum Sammeln von Informationen über die Aktivität dienen, durch.

Es sollte beachtet werden, dass laufend Informationen über die Aktivität des Benutzers im System gesammelt werden. Der Start einer beliebigen Datei oder das Öffnen eines Dokuments werden in einem Verlauf festgehalten, und das Systemjournal von Microsoft Windows registriert eine Vielzahl von Ereignissen, die im System vorfallen. Deshalb kann es sein, dass bei einem wiederholten Start des Assistenten zum Löschen von Aktivitätsspuren gefunden werden, die beim vorhergehenden Start des Assistenten bereits gelöscht worden sind. Es kann vorkommen, dass bestimmte Dateien, wie z.B. eine Journaldatei von Microsoft Windows, vom System verwendet werden, während sie vom Assistenten gelöscht werden sollen. Um diese Dateien zu löschen, schlägt der Assistent vor, das System neu zu starten. Im Verlauf eines Neustarts können solche Dateien aber erneut erstellt werden, was dazu führt, dass sie wieder als Aktivitätsspuren erkannt werden.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**. Zum Abschluss des Assistenten dient die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf **Abbrechen** abgebrochen werden.

Gehen Sie folgendermaßen vor, den Assistenten zum Löschen von Aktivitätsspuren zu starten:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Zusätzliche Funktionen**.
3. Klicken Sie im folgenden Fenster auf **Löschen von Aktivitätsspuren**.

Details zu den einzelnen Schritte des Assistenten

Schritt 1. Assistent starten

Vergewissern Sie sich, dass die Variante **Diagnose von Aktivitätsspuren des Benutzers** gewählt wurde, und klicken Sie auf **Weiter**, um den Assistenten zu starten.

Schritt 2. Suche von Aktivitätsspuren

Der Assistent führt auf Ihrem Computer die Suche nach Aktivitätsspuren aus. Die Suche kann eine gewisse Zeit beanspruchen. Der Assistent geht nach Abschluss der Suche automatisch zum nächsten Schritt.

Schritt 3. Aktionen für das Löschen von Aktivitätsspuren wählen

Nach dem Abschluss der Suche informiert der Assistent über die gefundenen Aktivitätsspuren und mögliche Aktionen, um sie zu beseitigen. Der Bericht über die Arbeit des Assistenten besitzt die Form einer Liste (s. Abschnitt "Zusätzliche Funktionen" auf S. 233).

Klicken Sie links vom Namen einer Gruppe auf das Zeichen **+**, um die Aktionen der Gruppe anzuzeigen.

Um eine bestimmte Aktion auszuführen, aktivieren Sie das Kontrollkästchen links vom Namen der Aktion. In der Grundeinstellung werden alle empfohlenen und ausdrücklich empfohlenen Aktionen ausgeführt. Soll eine bestimmte Aktion nicht ausgeführt werden, dann deaktivieren Sie das entsprechende Kontrollkästchen

Die standardmäßig aktivierten Kontrollkästchen sollten auf keinen Fall entfernt werden, weil dadurch die Sicherheit Ihres Computers bedroht wird.

Klicken Sie auf **Weiter**, nachdem Sie die Aktionen gewählt haben, die der Assistent ausführen soll.

Schritt 4. Aktivitätsspuren löschen

Der Assistent führt die Aktionen aus, die beim vorherigen Schritt festgelegt wurden. Das Löschen von Aktivitätsspuren kann eine gewisse Zeit beanspruchen. Um bestimmte Aktivitätsspuren zu löschen, kann ein Neustart des Computers erforderlich sein. Darüber werden Sie vom Assistenten informiert.

Der Assistent geht nach Abschluss des Löschens von Aktivitätsspuren automatisch zum nächsten Schritt.

Schritt 5. Assistent abschließen

Damit das Löschen von Aktivitätsspuren in Zukunft automatisch erfolgt, wenn Kaspersky PURE beendet wird, aktivieren Sie beim letzten Schritt des Assistenten das Kontrollkästchen **Löschen von Aktivitätsspuren jedes Mal beim Beenden von Kaspersky PURE ausführen**. Wenn Sie planen, die Aktivitätsspuren künftig selbst zu beseitigen, lassen Sie dieses Kontrollkästchen deaktiviert.

Klicken Sie auf die Schaltfläche **Beenden**, um den Assistenten abzuschließen.

NICHT VERWENDETE INFORMATIONEN LÖSCHEN

Im Betriebssystem sammeln sich im Lauf der Zeit temporäre oder nicht mehr verwendete Dateien an, was die Systemeffektivität verringert. Solche Dateien nehmen teilweise viel Speicherplatz in Anspruch und können außerdem von Schadprogrammen verwendet werden.

Temporäre Dateien werden beim Start von beliebigen Programmen und beim Hochfahren des Betriebssysytems erstellt. Beim Abschluss der Arbeit werden nicht alle temporären Dateien automatisch gelöscht.

Zu den nicht verwendeten Informationen werden folgende Dateien gezählt:

- Berichte über Systemereignisse, in denen die Namen aller geöffneten Programme protokolliert werden.
- Ereignisberichte unterschiedlicher Programme (z.B. Microsoft Office, Microsoft Visio, Macromedia Flash Player) oder Updatetools (z.B. Windows Updater, Adobe Updater)
- Berichte über Systemverbindungen
- temporäre Webbrowser-Dateien (Cookies)
- temporäre Dateien, die nach der Installation bzw. Deinstallation von Programmen zurückbleiben.
- Inhalt des Papierkorbs
- Dateien des Ordners TEMP, dessen Umfang mehrere Gigabyte erreichen kann.

Kaspersky PURE verfügt über einen Assistenten zum Löschen von nicht mehr benötigten Informationen. Die Aufgabe des Assistenten besteht darin, die Arbeit des Systems zu optimieren. Der Assistent löscht nicht nur die nicht mehr benötigten Dateien aus dem System, er entfernt auch Dateien, die vertrauliche Daten (Kennwörter, Benutzernamen und Informationen aus Anmeldeformularen) enthalten können. Trotzdem wird empfohlen, den Assistenten zum Löschen von Aktivitätsspuren (s. S. 235) zu verwenden, um solche Daten vollständig zu löschen.

Es kann sein, dass während der Systembereinigung bestimmte Dateien (z.B. Berichtsdatei von Microsoft Windows, Berichtsdatei für Microsoft Office) vom System verwendet werden. Um diese Dateien zu löschen, schlägt der Assistent vor, das System neu zu starten.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**. Zum Abschluss des Assistenten dient die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf **Abbrechen** abgebrochen werden.

Gehen Sie folgendermaßen vor, den Assistenten zum Löschen von nicht mehr verwendeten Informationen zu starten:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Zusätzliche Funktionen**.
3. Klicken Sie im folgenden Fenster auf **Löschen von nicht verwendeten Informationen**.

Details zu den einzelnen Schritte des Assistenten

Schritt 1. Assistent starten

Klicken Sie auf den Link **Weiter**, um den Assistenten zu starten.

Schritt 2. Nicht mehr verwendete Informationen suchen

Der Assistent sucht auf Ihrem Computer nach temporären und nicht mehr benötigten Dateien. Die Suche kann eine gewisse Zeit beanspruchen. Der Assistent geht nach Abschluss der Suche automatisch zum nächsten Schritt.

Schritt 3. Aktionen für das Löschen von nicht mehr benötigten Dateien auswählen

Nach dem Abschluss der Suche informiert der Assistent über die gefundenen, nicht mehr benötigten Dateien und über mögliche Aktionen, um diese zu löschen. Der Bericht über die Arbeit des Assistenten besitzt die Form einer Liste (s. Abschnitt "Zusätzliche Funktionen" auf S. 233).

Klicken Sie links vom Namen einer Gruppe auf das Zeichen **+**, um die Aktionen der Gruppe anzuzeigen.

Um eine bestimmte Aktion auszuführen, aktivieren Sie das Kontrollkästchen links vom Namen der Aktion. In der Grundeinstellung werden alle empfohlenen und ausdrücklich empfohlenen Aktionen ausgeführt. Soll eine bestimmte Aktion nicht ausgeführt werden, dann deaktivieren Sie das entsprechende Kontrollkästchen

Die standardmäßig aktivierten Kontrollkästchen sollten auf keinen Fall entfernt werden, weil dadurch die Sicherheit Ihres Computers bedroht wird.

Klicken Sie auf **Weiter**, nachdem Sie die Aktionen gewählt haben, die der Assistent ausführen soll.

Schritt 4. Nicht verwendete Informationen löschen

Der Assistent führt die Aktionen aus, die beim vorherigen Schritt festgelegt wurden. Das Löschen von nicht mehr benötigten Informationen kann eine gewisse Zeit beanspruchen. Um bestimmte nicht mehr benötigte Informationen zu löschen, kann ein Neustart des Computers erforderlich sein. Darüber werden Sie vom Assistenten informiert.

Der Assistent geht nach Abschluss des Löschens der nicht mehr benötigten Informationen automatisch zum nächsten Schritt.

Schritt 5. Assistent abschließen

Klicken Sie auf die Schaltfläche **Beenden**, um den Assistenten abzuschließen.

BROWSER-KONFIGURATION

In bestimmten Fällen ist es notwendig, den Browser Microsoft Internet Explorer auf spezielle Weise zu analysieren und anzupassen, da benutzerdefinierte oder standardmäßige Parameter zu Sicherheitsproblemen führen können.

Beispiele für Objekte und Parameter, die vom Browser verwendet werden und potentielle Sicherheitsrisiken bergen:

- **Zwischenspeicher für die Arbeit von Microsoft Internet Explorer**. Im Cache werden Daten gespeichert, die aus dem Internet heruntergeladen wurden. So lässt sich ein erneuter Download vermeiden. Dadurch wird die Ladedauer für Webseiten reduziert und der Internet-Datenverkehr verringert. Allerdings enthält der Zwischenspeicher vertrauliche Daten und kann außerdem Aufschluss darüber geben, welche Ressourcen ein Benutzer besucht hat. Viele schädliche Objekte lesen beim Scannen der Festplatte auch den Zwischenspeicher. Auf diese Weise können Angreifer beispielsweise die Mailadressen von Benutzern erhalten. Zur Optimierung des Schutzes wird empfohlen, den Zwischenspeicher zu leeren, wenn die Arbeit mit dem Browser beendet wird.

- **Anzeige von Erweiterungen für dem System bekannte Dateitypen**. Um das Umbenennen von Dateien zu erleichtern, können die Erweiterungen ausgeblendet werden. Allerdings ist es für den Benutzer manchmal besser, die tatsächliche Dateierweiterung zu sehen. Häufig werden in den Namen schädlicher Objekte Zeichenfolgen verwendet, in denen der echten Erweiterung zu Imitationszwecken eine zusätzliche Erweiterung vorangestellt wird (z.B. example.txt.com). Wenn die tatsächliche Dateierweiterung nicht angezeigt wird, sieht der Benutzer nur den Teil des Dateinamens, der die imitierte Erweiterung enthält, und kann das schädliche Objekt für eine unschädliche Datei halten. Zur Optimierung des Schutzes wird empfohlen, die Anzeige von Erweiterungen für Dateien bekannter Formate zu aktivieren.

- **Liste der vertrauenswürdigen Webseiten**. Um problemlos mit bestimmten Webseiten arbeiten zu können, müssen sie der vertrauenswürdigen Liste hinzugefügt werden. Allerdings können schädliche Objekte können einer solchen Liste Links zu Webseiten hinzufügen, die von Angreifern erstellt wurden.

Es sollte berücksichtigt werden, dass bestimmte Parameterwerte zu Problemen bei der Anzeige spezieller Webseiten führen können (beispielsweise wenn sie ActiveX-Elemente verwenden). Das Problem lässt sich lösen, indem solche Webseiten in die vertrauenswürdige Zone aufgenommen werden.

Die Analyse und Konfiguration wird vom Assistenten zur Browser-Konfiguration ausgeführt. Der Assistent prüft, ob die aktuellen Updates für den Browser installiert sind und ob die Browser-Einstellungen keine Schwachstellen aufweisen, die das System verletzbar machen. Beim Abschluss des Assistenten wird ein Bericht erstellt, der zur Analyse an Kaspersky Lab geschickt werden kann.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**. Zum Abschluss des Assistenten dient die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf **Abbrechen** abgebrochen werden.

Schließen Sie alle Browserfenster von Microsoft Internet Explorer, bevor mit der Diagnose begonnen wird.

Gehen Sie folgendermaßen vor, den Assistenten zur Browser-Konfiguration zu starten:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Fensterbereich auf **Zusätzliche Funktionen**.
3. Klicken Sie im folgenden Fenster auf **Browser für sichere Arbeit anpassen**.

Details zu den einzelnen Schritte des Assistenten

Schritt 1. Assistent starten

Vergewissern Sie sich, dass die Variante **Diagnose von Microsoft Internet Explorer** gewählt wurde, und klicken Sie auf **Weiter**, um den Assistenten zu starten.

Schritt 2. Analyse der Einstellungen von Microsoft Internet Explorer

Der Assistent analysiert die Einstellungen des Browsers Microsoft Internet Explorer. Die Suche nach Problemen in den Einstellungen des Browsers kann eine gewisse Zeit beanspruchen. Der Assistent geht nach Abschluss der Suche automatisch zum nächsten Schritt.

Schritt 3. Aktionen für die Browser-Konfiguration wählen

Alle Probleme, die beim vorherigen Schritt gefunden wurden, werden im Hinblick auf ihre Gefährlichkeit für das System (s. Abschnitt "Zusätzliche Funktionen" auf S. 233) eingeteilt.

Klicken Sie links vom Namen einer Gruppe auf das Zeichen **+**, um die Aktionen der Gruppe anzuzeigen.

Um eine bestimmte Aktion auszuführen, aktivieren Sie das Kontrollkästchen links vom Namen der Aktion. In der Grundeinstellung werden alle empfohlenen und ausdrücklich empfohlenen Aktionen ausgeführt. Soll eine bestimmte Aktion nicht ausgeführt werden, dann deaktivieren Sie das entsprechende Kontrollkästchen

Die standardmäßig aktivierten Kontrollkästchen sollten auf keinen Fall entfernt werden, weil dadurch die Sicherheit Ihres Computers bedroht wird.

Klicken Sie auf **Weiter**, nachdem Sie die Aktionen gewählt haben, die der Assistent ausführen soll.

Schritt 4. Browser-Konfiguration

Der Assistent führt die Aktionen aus, die beim vorherigen Schritt festgelegt wurden. Die Browser-Konfiguration kann eine gewisse Zeit beanspruchen. Der Assistent geht nach Abschluss der Konfiguration automatisch zum nächsten Schritt.

Schritt 5. Assistent abschließen

Klicken Sie auf die Schaltfläche **Beenden**, um den Assistenten abzuschließen.

BERICHTE

Die Ereignisse, die während der Arbeit der Schutzkomponenten oder bei der Ausführung von Aufgaben von Kaspersky PURE eintreten, werden in Berichten festgehalten. Sie können für jede Schutzkomponente oder Aufgabe einen detaillierten Bericht erstellen und die Darstellung der Daten anpassen. Außerdem können Sie die Daten filtern (s. Abschnitt "Datenfilterung" auf S. 240) und in einem Bericht nach Ereignissen suchen (s. Abschnitt "Suche nach Ereignissen" auf S. 241).

Falls erforderlich, können Sie die Daten eines Berichts in einer Textdatei speichern (s. Abschnitt "Bericht in Datei speichern" auf S. 242). Außerdem können Sie die Berichte, deren Daten Sie nicht mehr benötigen, leeren (s. Abschnitt "Berichte leeren" auf S. 243) und die Parameter für das Erstellen (s. Abschnitt "Nicht kritische Ereignisse protokollieren" auf S. 243) und Speichern von Berichten (s. Abschnitt "Berichte speichern" auf S. 242) anpassen.

IN DIESEM ABSCHNITT

Bericht für eine bestimmte Komponente erstellen 240

Datenfilterung 240

Suche nach Ereignissen 241

Bericht in Datei speichern 242

Berichte speichern 242

Berichte leeren 243

Nicht kritische Ereignisse protokollieren 243

Erinnerung an die Bereitschaft eines Berichts anpassen 243

BERICHT FÜR EINE BESTIMMTE KOMPONENTE ERSTELLEN

Sie können einen detallierten Bericht über die Ereignisse erhalten, die bei der Arbeit der einzelnen Komponenten und Aufgaben von Kaspersky PURE eintreten.

Zur übersichtlichen Arbeit mit Berichten können Sie die Darstellung von Daten auf dem Bildschirm ändern: Ereignisse nach unterschiedlichen Parametern anordnen, Berichtszeitraum wählen, Ereignisse nach einer Spalte oder nach Priorität anordnen, Tabellenspalten ausblenden.

Gehen Sie folgendermaßen vor, um einen Bericht für eine Komponente oder Aufgabe zu erhalten:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.

   Das Fenster **Computersicherheit** wird geöffnet.

2. Gehen Sie mit Hilfe des Links **Bericht** in das Berichtsfenster von Kaspersky PURE.

3. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf **Detaillierter Bericht**.

   Das Fenster **Detaillierter Bericht** wird geöffnet.

4. Wählen Sie aus der Dropdown-Liste links oben eine Komponente oder Aufgabe aus, für die ein Bericht erstellt werden soll. Bei Auswahl des Punkts **Schutz-Center** wird ein Bericht für alle Schutzkomponenten erstellt.

DATENFILTERUNG

Die Ereignisse in den Berichten für Kaspersky PURE können nach einem oder mehreren Werten in den Tabellenspalten gefiltert werden. Außerdem lassen sich komplexe Bedingungen für die Datenfilterung festlegen.

Gehen Sie folgendermaßen vor, um die Ereignisse nach Werten zu filtern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.

   Das Fenster **Computersicherheit** wird geöffnet.

2. Gehen Sie mit Hilfe des Links **Bericht** in das Berichtsfenster von Kaspersky PURE.

3. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf **Detaillierter Bericht**.

Das Fenster **Detaillierter Bericht** wird geöffnet.

4. Zeigen Sie im rechten Fensterbereich mit der Maus auf die linke obere Ecke der Überschrift einer Tabellenspalte und öffnen Sie durch Linksklick das Filtermenü.

5. Wählen Sie im Filtermenü den Wert, nach dem die Daten gefiltert werden sollen.

6. Wiederholen Sie den Vorgang bei Bedarf für eine andere Tabellenspalte.

Gehen Sie folgendermaßen vor, um eine komplexe Filterbedingung festzulegen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.

   Das Fenster **Computersicherheit** wird geöffnet.

2. Gehen Sie mit Hilfe des Links **Bericht** in das Berichtsfenster von Kaspersky PURE.

3. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf **Detaillierter Bericht**.

   Das Fenster **Detaillierter Bericht** wird geöffnet.

4. Öffnen Sie im rechten Fensterbereich durch Rechtsklick das Kontextmenü für die entsprechende Berichtspalte und wählen Sie dort den Punkt **Filter**.

5. Legen Sie im folgenden Fenster **Komplexer Filter** die Filterbedingungen fest.

   a. Legen Sie auf der rechten Fensterseite die Auswahlgrenzen fest.

   b. Wählen Sie auf der linken Fensterseite in der Dropdown-Liste **Bedingung** eine Auswahlbedingung fest (z.B.: größer oder kleiner, gleich oder ungleich mit dem Wert, der als Auswahlgrenze angegeben wurde).

   c. Fügen Sie bei Bedarf eine zweite Bedingung hinzu. Verwenden Sie dazu die logischen Operationen Konjunktion (logisches UND) und Disjunktion (logisches ODER). Wenn Sie möchten, dass er Datenzugriff beide festgelegte Bedingungen erfüllt, wählen Sie **UND**. Ist eine Bedienung ausreichend, dann wählen Sie **ODER**.

SUCHE NACH EREIGNISSEN

Um in einem Bericht nach einem bestimmten Ereignis zu suchen, können Sie entweder in der Suchzeile oder in einem speziellen Fenster ein Schlüsselwort eingeben.

Gehen Sie folgendermaßen vor, um nach einem Ereignis zu suchen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.

   Das Fenster **Computersicherheit** wird geöffnet.

2. Gehen Sie mit Hilfe des Links **Bericht** in das Berichtsfenster von Kaspersky PURE.

3. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf **Detaillierter Bericht**.

   Das Fenster **Detaillierter Bericht** wird geöffnet.

4. Öffnen Sie durch Rechtsklick das Kontextmenü für die Überschrift der entsprechenden Spalte und wählen Sie dort den Punkt **Suche** aus.

5. Legen Sie im folgenden **Fenster** Suche die Suchkriterien fest.

   a. Geben Sie im Feld **Zeile** das gesuchte Schlüsselwort ein.

b. Wählen Sie in der Dropdown-Liste **Spalte** den Namen der Spalte, in der nach dem angegebenen Schlüsselwort gesucht werden soll.

c. Aktivieren Sie bei Bedarf die Kontrollkästchen für zusätzliche Suchparameter.

6. Klicken Sie auf **Weitersuchen**.

BERICHT IN DATEI SPEICHERN

Der Bericht kann in einer Textdatei gespeichert werden.

Gehen Sie folgendermaßen vor, um den Bericht in einer Datei zu speichern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.

   Das Fenster **Computersicherheit** wird geöffnet.

2. Gehen Sie mit Hilfe des Links **Bericht** in das Berichtsfenster von Kaspersky PURE.

3. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf **Detaillierter Bericht**.

   Das Fenster **Detaillierter Bericht** wird geöffnet.

4. Erstellen Sie den gewünschten Bericht und klicken Sie auf **Speichern**.

5. Geben Sie im folgenden Fenster den Ordner an, in dem die Berichtsdatei gespeichert werden soll, und nennen Sie einen Dateinamen.

BERICHTE SPEICHERN

Die standardmäßige Speicherdauer für Ereignisberichte beträgt 30 Tage. Danach werden die Daten gelöscht. Sie können diese Zeitbeschränkung aufheben oder die maximale Speicherdauer für Berichte ändern.

Außerdem können Sie eine maximale Größe für eine Berichtsdatei festlegen. Die maximale Größe beträgt standardmäßig 1024 MB. Beim Erreichen der maximalen Größe wird der Inhalt der Datei durch neue Einträge ersetzt. Sie können die Größenbeschränkung aufheben oder einen anderen Wert festlegen.

Gehen Sie folgendermaßen vor, um eine maximale Speicherdauer für Ereignisberichte festzulegen:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie auf der linken Fensterseite im Abschnitt **Allgemeine Einstellungen** den Abschnitt **Berichte und Speicher**.

4. Aktivieren Sie auf der rechten Fensterseite im Block **Speichern** das Kontrollkästchen **Berichte speichern für maximal** und legen Sie eine maximale Speicherdauer für Berichte fest.

Gehen Sie folgendermaßen vor, um die maximale Größe einer Berichtsdatei festzulegen:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.

3. Wählen Sie auf der linken Fensterseite im Abschnitt **Allgemeine Einstellungen** den Abschnitt **Berichte und Speicher**.

4. Aktivieren Sie auf der rechten Fensterseite im Block **Speichern** das Kontrollkästchen **Maximale Dateigröße** und legen Sie die maximale Größe einer Berichtsdatei fest.

BERICHTE LEEREN

Berichte, deren Daten Sie nicht mehr benötigen, können bereinigt werden.

Um die Berichte zu leeren*, machen Sie Folgendes*:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Allgemeine Einstellungen** den Abschnitt **Berichte und Speicher**.
4. **Klicken Sie auf der rechten Fensterseite im Block** Berichte leeren auf **Leeren**.
5. Aktivieren Sie im folgenden Fenster **Informationen aus Berichten löschen** die Kontrollkästchen der Berichte, die Sie bereinigen möchten.

NICHT KRITISCHE EREIGNISSE PROTOKOLLIEREN

Einträge über nicht kritische Ereignisse sowie Ereignisse, die die Registrierung und das Dateisystem betreffen, werden in der Grundeinstellung nicht protokolliert. Sie können solche Einträge in den Schutzbericht aufnehmen.

Gehen Sie folgendermaßen vor, um die Protokollierung von nicht kritischen Ereignissen zu aktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Allgemeine Einstellungen** den Abschnitt **Berichte und Speicher**.
4. Aktivieren Sie im rechten Fensterbereich im Block **Protokollierte Ereignisse** die Kontrollkästchen für die zu protokollierenden Ereignistypen.

ERINNERUNG AN DIE BEREITSCHAFT EINES BERICHTS ANPASSEN

Sie können einen Zeitplan erstellen, nach dem Kaspersky PURE Sie über die Bereitschaft eines Berichts benachrichtigen soll.

Gehen Sie folgendermaßen vor, um einen Zeitplan zu erstellen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf **Computersicherheit**.

   Das Fenster **Computersicherheit** wird geöffnet.
2. Gehen Sie mit Hilfe des Links **Bericht** in das Berichtsfenster von Kaspersky PURE.
3. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Bericht** das Kontrollkästchen **An Bericht erinnern** und klicken Sie auf den Link mit dem eingestellten Zeitpunkt, um das Zeitplanfenster zu öffnen.
4. Stellen Sie im folgenden Fenster **Bericht: Zeitplan** den Zeitplan ein.

MELDUNGEN

Standardmäßig werden Sie beim Auftreten von Ereignissen während der Ausführung von Kaspersky PURE entsprechend informiert. Wenn Sie über das weitere Vorgehen entscheiden sollen, erscheinen auf dem Bildschirm Meldungsfenster (s. Abschnitt "Meldungsfenster und Popupmeldungen" auf S. 56). Über Ereignisse, die keine Auswahl des weiteren Vorgehens erfordern, informiert das Programm mit Hilfe von akustischen Signalen, E-Mails und Popupmeldungen im Infobereich der Taskleiste (s. Abschnitt "Meldungsfenster und Popupmeldungen" auf S. 56).

Sie können für die Ereignisse eine Benachrichtigungsmethode (s. Abschnitt "Benachrichtigungsmethode anpassen" auf S. 244) wählen oder das Senden von Benachrichtigungen (s. Abschnitt "Benachrichtigungen aktivieren und deaktivieren" auf S. 244).

SIEHE AUCH:

Benachrichtigungsmethode anpassen 244

BENACHRICHTIGUNGEN AKTIVIEREN UND DEAKTIVIEREN

Standardmäßig benachrichtigt Sie Kaspersky PURE auf verschiedene Arten über wichtige Ereignisse im Zusammenhang mit der Ausführung des Programms (s. Abschnitt "Benachrichtigungsmethode anpassen" auf S. 244). Sie können das Senden von Benachrichtigungen deaktivieren.

Die Informationen über Ereignisse, die während der Ausführung von Kaspersky PURE auftreten, werden unabhängig davon, ob die Benachrichtigungen aktiviert oder deaktiviert sind, im Bericht über die Programmarbeit protokolliert.

Die Deaktivierung der Benachrichtigungen hat keinen Einfluss auf die Anzeige der Meldungsfenster. Um nur eine minimale Anzahl an Meldungsfenstern auf dem Bildschirm anzeigen zu lassen, verwenden Sie den automatischen Schutzmodus (s. Abschnitt "Schutzmodus auswählen" auf S. 61).

Gehen Sie folgendermaßen vor, um den Versand von Benachrichtigungen zu aktivieren oder zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Allgemeine Einstellungen** den Abschnitt **Meldungen**.
4. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Ereignisse melden**, um den Versand von Benachrichtigungen zu auszuschalten. Aktivieren Sie dieses Kontrollkästchen, um den Versand von Benachrichtigungen einzuschalten.

BENACHRICHTIGUNGSMETHODE ANPASSEN

Das Programm informiert Sie auf folgende Arten über Ereignisse:

- durch Popupmeldungen im Infobereich der Taskleiste;
- durch ein akustisches Signal;
- per E-Mail.

Die können die Benachrichtigungsmethoden für jede Art von Ereignis individuell einstellen.

Kritische Meldungen und Meldungen über Störungen des Programms werden standardmäßig von akustischen Signalen begleitet. Für die Audiosignale wird das Soundschema Microsoft Windows verwendet. Sie können ein anderes Schema wählen oder die Tonsignale ausschalten.

Gehen Sie wie folgt vor, um die Benachrichtigungsmethoden für die verschiedenen Ereignistypen zu konfigurieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Allgemeine Einstellungen** den Abschnitt **Meldungen**.
4. Aktivieren Sie im rechten Fensterbereich das Kontrollkästchen **Ereignisse melden** und klicken Sie rechts auf **Einstellungen**.
5. Aktivieren Sie im erscheinenden Fenster **Meldungen** die Kontrollkästchen je nachdem, wie Sie Ihre Benachrichtigungen über die verschiedenen Ereignisse erhalten möchten: per E-Mail, in Form von Popupmeldungen oder per akustischem Signal. Um für einen bestimmten Ereignistyp keinerlei Benachrichtigungen zu erhalten, müssen Sie alle Kontrollkästchen in der Zeile dieses Ereignisses deaktivieren.

   Damit Kaspersky PURE Sie per E-Mail über Ereignisse benachrichtigen kann, müssen Sie die entsprechenden Einstellungen für die Zustellung per E-Mail vornehmen.

Gehen Sie folgendermaßen vor, um die E-Mail-Parameter für das Senden von Meldungen anzupassen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Allgemeine Einstellungen** den Abschnitt **Meldungen**.
4. Aktivieren Sie im rechten Fensterbereich das Kontrollkästchen **E-Mails über Ereignisse senden** und klicken Sie rechts auf **Einstellungen**.
5. Geben Sie im folgenden Fenster **E-Mail-Meldungen anpassen** die Versandparameter an.

Gehen Sie folgendermaßen vor, um das Soundschema zu ändern:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Allgemeine Einstellungen** den Abschnitt **Meldungen**.
4. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Standardsoundschema Windows Default verwenden** und das vom Betriebssystem verwendete Schema.

   Wenn das Kontrollkästchen deaktiviert ist, wird das Soundschema der vorhergehenden Programmversion verwendet.

Gehen Sie folgendermaßen vor, um die Audiosignale zur Begleitung von Benachrichtigungen zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Allgemeine Einstellungen** den Abschnitt **Meldungen**.
4. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Audiosignale für Meldungen aktivieren**.

TEILNAHME AN KASPERSKY SECURITY NETWORK

Jeden Tag taucht eine Vielzahl neuer Bedrohungen auf. Um ein schnelles Sammeln von Informationen über die Typen und Quellen neuer Bedrohungen zu gewährleisten und die Entwicklung entsprechender Neutralisierungsmethoden zu beschleunigen, können Sie sich dem Kaspersky Security Network anschließen.

Kaspersky Security Network (KSN) ist eine Infrastruktur der Online-Dienste und -Services, die den Zugriff auf die aktuelle Wissensdatenbank von Kaspersky Lab über den "Ruf" der Dateien, Internet-Ressourcen und Programme bietet. Durch die Verwendung der Daten von Kaspersky Security Network wird die Geschwindigkeit der Reaktion von Kaspersky PURE auf neue Bedrohungen und die Leistungsfähigkeit einiger Komponenten erhöht. Außerdem wird dadurch das Risiko verringert, dass Fehlalarme auftreten.

Bei Teilnahme am Kaspersky Security Network wird eine Statistik, die während der Arbeit von Kaspersky PURE auf Ihrem Computer erstellt wird, automatisch an Kaspersky Lab übermittelt.

Es werden keine persönlichen Daten gesammelt, verarbeitet oder gespeichert.

Die Teilnahme an Kaspersky Security Network ist freiwillig. In der Regel entscheiden Sie im Verlauf der Installation von Kaspersky PURE über die Teilnahme. Allerdings können Sie Ihre Entscheidung jederzeit ändern.

Gehen Sie folgendermaßen vor, um die Verwendung von Kaspersky Security Network zu aktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf den Link **Einstellungen**.
3. Wählen Sie auf der linken Fensterseite im Abschnitt **Allgemeine Einstellungen** den Abschnitt **Feedback**.
4. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Ich akzeptiere die Teilnahmebedingungen für Kaspersky Security Network**.

EINSTELLUNGEN VON KASPERSKY PURE AUF KORREKTHEIT PRÜFEN

Nach der Installation und Konfiguration von Kaspersky PURE können Sie mit Hilfe eines "Testvirus" und dessen Modifikationen prüfen, ob die Einstellungen korrekt sind. Die Prüfung muss für jede Schutzkomponente und für jedes Protokoll einzeln ausgeführt werden.

In diesem Abschnitt

EICAR-"Testvirus" und seine Modifikationen 247

Testen des Schutzes für HTTP-Datenverkehr 249

Schutz für den SMTP-Datenverkehr testen 249

Überprüfung der Einstellungen von Datei-Anti-Virus 249

Überprüfung der Einstellungen für eine Aufgabe zur Virensuche 250

Überprüfung der Einstellungen für den Schutz vor unerwünschten E-Mails 250

EICAR-"Testvirus" und seine Modifikationen

Dieser "Testvirus" wurde vom Institut EICAR (The European Institute for Computer Antivirus Research) speziell zum Überprüfen der Arbeit von Antiviren-Produkten entwickelt.

Der Testvirus IST KEINE Schadsoftware und enthält keinen Programmcode, der Ihrem Computer Schaden zuzufügen könnte. Dennoch wird EICAR von den meisten Produkten der Entwickler von Virenschutzsoftware als Virus erkannt.

Verwenden Sie nie echte Viren, um die Funktionsfähigkeit eines Antiviren-Produkts zu testen!

Der "Testvirus" kann von der offiziellen Internetseite des EICAR-Instituts heruntergeladen werden: http://www.eicar.org/anti_virus_test_file.htm.

Vor dem Download muss der Antiviren-Schutz deaktiviert werden, weil der von der Seite anti_virus_test_file.htm heruntergeladene Testvirus andernfalls als infiziert erkannt und vom Programm als infiziertes, per HTTP-Protokoll übertragenes Objekt behandelt wird.

Die von der Webseite des EICAR-Instituts heruntergeladene Datei wird vom Programm als infiziertes Objekt identifiziert, das einen Virus enthält, der nicht desinfiziert werden kann, und führt die für diesen Objekttyp festgelegte Aktion aus.

Um die Funktion des Programms zu prüfen, können Sie auch Modifikationen des standardmäßigen "Testvirus" verwenden. Dazu wird der Inhalt des standardmäßigen "Testvirus" durch das Hinzufügen eines bestimmten Präfixes geändert (siehe Tabelle unten). Zum Erstellen von Modifikationen des "Testvirus" eignet sich ein beliebiger Text-Editor oder Hypertext-Editor wie beispielsweise Microsoft Editor, UltraEdit32, usw.

Die erste Spalte der Tabelle (s. unten) enthält Präfixe, die dem Standard-Testvirus zur Erzeugung einer Modifikation am Zeilenanfang hinzugefügt werden müssen. Die zweite Spalte zeigt die möglichen Werte für den Status, der einem Objekt aufgrund der Untersuchungsergebnisse zugewiesen werden kann. Die dritte Spalte bietet Informationen darüber, wie Objekte mit dem betreffenden Status vom Programm bearbeitet werden. Beachten Sie, dass die Aktionen für Objekte durch die Werte der Programmparameter bestimmt werden.

Nach Hinzufügen des Präfixes zum Testvirus speichern Sie die so entstandene Datei unter einem Namen, der eine Vorstellung von der Modifikationen des Virus vermittelt: Wenn Sie beispielsweise das Präfix DELE- hinzugefügt haben, bietet es sich an, die entstandene Datei unter dem Namen eicar_dele.com zu speichern.

Vergessen Sie nicht, den Virenschutz nach dem Download des Testvirus und der Herstellung der Modifikationen zu aktualisieren.

Tabelle 2. Modifikationen des "Testvirus"

Präfix	Status des Objekts	Informationen zur Verarbeitung des Objekts
Kein Präfix, standardmäßiger "Testvirus".	**Infiziert**. Das Objekt enthält einen bekannten Viruscode. Die Desinfektion ist nicht möglich.	Das Programm identifiziert dieses Objekt als Virus, der nicht desinfiziert werden kann. Beim Desinfektionsversuch des Objekts tritt ein Fehler auf und die für irreparable Objekte geltende Aktion wird ausgeführt.
CORR-	**Beschädigt**.	Das Programm hat Zugriff auf das Objekt erhalten, kann es aber aufgrund einer Beschädigung nicht untersuchen (z.B. beschädigte Struktur des Objekts, ungültiges Dateiformat). Informationen darüber, dass das Objekt verarbeitet wurde, können Sie dem Bericht über die Arbeit der Anwendung entnehmen.
WARN-	**Verdächtig**. Das Objekt enthält einen unbekannten Viruscode. Die Desinfektion ist nicht möglich.	Das Objekt wurde als verdächtig erkannt. Im Augenblick des Funds enthalten die Programm-Datenbanken keine Beschreibung zur Desinfektion dieses Objekts. Beim Fund eines solchen Objekts, erhalten Sie eine Meldung.
SUSP-	**Verdächtig**. Das Objekt enthält den modifizierten Code eines bekannten Virus. Die Desinfektion ist nicht möglich.	Das Programm hat erkannt, dass der Objektcode teilweise mit dem Code eines bekannten Virus übereinstimmt. Im Augenblick des Funds enthalten die Programm-Datenbanken keine Beschreibung zur Desinfektion dieses Objekts. Beim Fund eines solchen Objekts, erhalten Sie eine Meldung.
ERRO-	**Untersuchungsfehler**.	Bei der Untersuchung des Objekts ist ein Fehler aufgetreten. Die Anwendung erhielt keinen Zugriff auf das Objekt: Die Integrität des Objekts ist beschädigt (z.B. kein Endpunkt in einem Multi-Level-Archiv) oder die Verbindung zu dem Objekt fehlt (wenn ein Objekt in einer Netzwerkressource untersucht wird). Informationen darüber, dass das Objekt verarbeitet wurde, können Sie dem Bericht über die Arbeit der Anwendung entnehmen.
CURE-	**Infiziert**. Das Objekt enthält einen bekannten Viruscode. Die Desinfektion ist möglich.	Das Objekt enthält einen Virus, der desinfiziert werden kann. Das Programm führt die Desinfektion des Objekts aus, wobei der Text des Viruskörpers in CURE geändert wird. Beim Fund eines solchen Objekts, erhalten Sie eine Meldung.
DELE-	**Infiziert**. Das Objekt enthält einen bekannten Viruscode. Die Desinfektion ist nicht möglich.	Das Programm identifiziert dieses Objekt als Virus, der nicht desinfiziert werden kann. Beim Desinfektionsversuch des Objekts tritt ein Fehler auf und die für irreparable Objekte geltende Aktion wird ausgeführt. Beim Fund eines solchen Objekts, erhalten Sie eine Meldung.

TESTEN DES SCHUTZES FÜR HTTP-DATENVERKEHR

Gehen Sie folgendermaßen vor, um die den Virenschutz für den mit HTTP-Protokoll übertragenen Datenverkehr zu prüfen:

Versuchen Sie, den "Testvirus" von der offiziellen Internetseite des **EICAR**-Instituts herunterzuladen: http://www.eicar.org/anti_virus_test_file.htm.

Beim Versuch, den "Testvirus" herunterzuladen, erkennt Kaspersky PURE das Objekt, identifiziert es als infiziert und irreparabel, und führt die Aktion aus, die in den Einstellungen für die Untersuchung des HTTP-Datenverkehrs dafür festgelegt wurde. Wenn versucht wird, den "Testvirus" herunterzuladen, wird in der Grundeinstellung die Verbindung mit der Ressource getrennt und im Browserfenster erscheint eine Meldung darüber, dass dieses Objekt von dem Virus EICAR-Test-File infiziert ist.

SCHUTZ FÜR DEN SMTP-DATENVERKEHR TESTEN

Um den Virenschutz für den mit SMTP-Protokoll übertragenen Datenverkehr zu prüfen, können Sie ein Mailprogramm verwenden, das die Daten mit diesem Protokoll überträgt.

Es wird empfohlen, die Virenerkennung in verschiedenen Teilen ausgehender Nachrichten zu testen, sowohl im Nachrichtenkörper als auch in den Anlagen. Verwenden Sie zu Testzwecken die Datei des EICAR-Testvirus (s. Abschnitt "EICAR-"Testvirus" und seine Modifikationen" auf S. 247).

Zum Testen der Virenerkennung in einem per SMTP-Protokoll versandten Datenstrom gehen Sie wie folgt vor:

1. Erstellen Sie mit Hilfe des auf Ihrem Computer installierten Mailprogramms eine E-Mail im Format Gewöhnlicher Text.

   Eine Nachricht, die den "Testvirus" enthält und das Format RTF oder HTML besitzt, wird nicht untersucht!

2. Führen Sie abhängig davon, in welchem Teil der Nachricht der Virus gefunden werden soll, folgende Aktionen aus:

   - Fügen Sie für den Fund des Virus im Nachrichtenkörper den Text des Standard-EICAR-Testvirus oder eines modifizierten EICAR-Testvirus am Anfang der Nachricht ein.
   - Für einen Virenfund in den Anhängen hängen Sie an die Nachricht eine Datei mit dem EICAR-Testvirus an.

3. Schicken Sie die E-Mail an die Adresse des Administrators.

Das Programm erkennt das Objekt, identifiziert es als infiziert und blockiert das Senden der E-Mail.

ÜBERPRÜFUNG DER EINSTELLUNGEN VON DATEI-ANTI-VIRUS

Gehen Sie folgendermaßen vor, um zu prüfen, ob Datei-Anti-Virus korrekt eingestellt wurde:

1. Erstellen Sie einen Ordner auf der Festplatte. Kopieren Sie den von der offiziellen Seite des **EICAR**-Instituts (http://www.eicar.org/anti_virus_test_file.htm) heruntergeladenen "Testvirus" und die von Ihnen erstellten Modifikationen des "Testvirus" in diesen Ordner.

2. Erlauben Sie das Protokollieren aller Ereignisse, damit Daten über beschädigte Objekte oder Objekte, die aufgrund einer Störung nicht untersucht werden, in der Berichtsdatei gespeichert werden.

3. Starten Sie den "Testvirus" oder seine Modifikation zur Ausführung.

Datei-Anti-Virus fängt den Zugriff auf die Datei ab, untersucht sie und führt die in den Einstellungen festgelegte Aktion aus. Durch die Auswahl unterschiedlicher Aktionsvarianten für ein gefundenes Objekt können Sie die Funktion der Komponente vollständig testen.

Vollständige Informationen über die Arbeitsergebnisse von Datei-Anti-Virus sind im Bericht über die Arbeit der Komponente enthalten.

ÜBERPRÜFUNG DER EINSTELLUNGEN FÜR EINE AUFGABE ZUR VIRENSUCHE

Gehen Sie folgendermaßen vor, um zu prüfen, ob eine Aufgabe zur Virensuche korrekt eingestellt wurde:

1. Erstellen Sie einen Ordner auf der Festplatte. Kopieren Sie den von der offiziellen Seite des EICAR-Instituts **EICAR** (http://www.eicar.org/anti_virus_test_file.htm) heruntergeladenen "Testvirus" und die von Ihnen erstellten Modifikationen des "Testvirus" in diesen Ordner.

2. Erstellen Sie eine neue Untersuchungsaufgabe und wählen Sie als Untersuchungsobjekt den Ordner, der die "Testviren" enthält.

3. Erlauben Sie das Protokollieren aller Ereignisse, damit Daten über beschädigte Objekte oder Objekte, die aufgrund einer Störung nicht untersucht werden, in der Berichtsdatei gespeichert werden.

4. Starten Sie die Ausführung der Untersuchungsaufgabe.

Wenn bei der Untersuchung verdächtige oder infizierte Objekte gefunden werden, werden die in den Einstellungen der Aufgabe festgelegten Aktionen ausgeführt. Durch die Auswahl unterschiedlicher Aktionsvarianten für ein gefundenes Objekt können Sie die Funktion der Komponente vollständig testen.

Vollständige Informationen über das Ausführungsergebnis der Untersuchungsaufgabe sind im Bericht über die Arbeit der Komponente enthalten.

ÜBERPRÜFUNG DER EINSTELLUNGEN FÜR DEN SCHUTZ VOR UNERWÜNSCHTEN E-MAILS

Zur Überprüfung des Schutzes vor unerwünschten E-Mails können Sie eine Testnachricht verwenden, die vom Programm als Spam identifiziert wird.

Die Testnachricht muss folgenden Text in der Betreffzeile enthalten:

```
Spam is bad do not send it
```

Nachdem diese Nachricht auf dem Computer eingetroffen ist, untersucht Kaspersky PURE sie, stuft sie als Spam ein und führt die Aktion damit aus, die für diesen Objekttyp festgelegt wurde.

KONTAKTAUFNAHME MIT DEM TECHNISCHEN SUPPORT

Wenn bei der Verwendung von Kaspersky PURE Probleme auftreten sollten, prüfen Sie zuerst, ob die Dokumentation, die Hilfe, die Wissensdatenbank auf der Seite des Technischen Supports von Kaspersky Lab oder das Benutzerforum keine Lösung dafür bieten.

Wenn Sie keine Lösung für Ihr Problem finden können, wenden Sie sich an den Technischen Support von Kaspersky Lab. Dies ist auf folgende Weise möglich:

- aus Mein Kaspersky Account eine Anfrage an die Webseite des Technischen Supports senden.
- telefonisch

Die Spezialisten des Technischen Supports beantworten Ihre Fragen zur Installation, Aktivierung und Verwendung des Programms. Wenn Ihr Computer infiziert wurde, helfen sie Ihnen dabei, die Folgen der schädlichen Malware-Aktionen zu beheben.

Bevor Sie sich an den Technischen Support wenden, lesen Sie sich bitte zuvor die Supportrichtlinien (http://support.kaspersky.ru/support/rules) durch.

Wenn Sie sich an den Technischen Support wenden, bitten die Support-Experten Sie möglicherweise darum, einen Bericht über den Systemzustand und eine Protokolldatei zu erstellen und diese an den Technischen Support zu senden. Aufgrund einer Analyse der von Ihnen eingesandten Daten können die Support-Experten ein AVZ-Skript erstellen, das an Sie geschickt wird. Mit diesem Skript können Sie die aufgetretenen Probleme beheben.

In diesem Abschnitt

Mein Kaspersky Account 251

Technischer Support am Telefon 252

Bericht über den Systemstatus erstellen 252

Protokolldatei erstellen 253

Dateien mit Daten senden 253

AVZ-Skript ausführen 254

Mein Kaspersky Account

Mein Kaspersky Account ist Ihr persönlicher Bereich auf der Seite des Technischen Supports. Dort können Sie folgende Aktionen ausführen:

- Anfragen an den Technischen Support und an das Virenlabor senden.
- ohne E-Mail mit dem Technischen Support kommunizieren.
- Status Ihrer Anfragen in Echtzeit verfolgen.
- Verlauf Ihrer Zugriffe auf den Technischen Support ansehen.

Verwenden Sie eine der folgenden Methoden, um die Login-Seite für den persönlichen Bereich zu öffnen:

- Verwenden Sie den Link **Mein Kaspersky Account** im Hauptfenster von Kaspersky PURE.
- Geben Sie in der Adressenleiste des Browsers ein: .

Wenn Sie noch keinen Kaspersky Account besitzen, können Sie auf die Registrierungsseite https://my.kaspersky.com/de/registration gehen. Geben Sie hier Ihre E-Mail-Adresse und ein Kennwort für den Zugriff auf Ihren Kaspersky Account an. Für Anfragen zu Kaspersky PURE benötigen Sie den Aktivierungscode des Programms.

Beachten Sie, dass bestimmte Anfragen nicht an den Technischen Support, sondern an das Virenlabor gerichtet werden müssen. Dazu zählen folgende Arten von Anfragen:

- unbekanntes Schadprogramm – Sie haben den Verdacht, dass ein bestimmtes Objekt schädlich ist, obwohl Kaspersky PURE es nicht als Malware einstuft.
- Viren-Fehlalarm – Kaspersky PURE stuft eine bestimmte Datei als infiziert ein, während Sie sicher sind, dass die Datei virenfrei ist.
- Anfrage für eine Beschreibung eines Schadprogramms – Sie möchten die Beschreibung eines bestimmten Virus erhalten.

Für Anfragen an das Virenlabor ist kein Aktivierungscode erforderlich.

Anfragen an das Virenlabor können Sie auf der Seite (http://support.kaspersky.ru/virlab/helpdesk.html?LANG=de) stellen.

TECHNISCHER SUPPORT AM TELEFON

Zur Lösung dringender Probleme können Sie jederzeit Ihren lokalen Technischen Support anrufen. Bevor Sie sich an die Fachleute vom deutschsprachigen oder internationalen technischen Support wenden, tragen Sie bitte Daten über Ihren Computer und das installierte Antiviren-Produkt zusammen. Dadurch können unsere Spezialisten Ihnen möglichst schnell helfen.

BERICHT ÜBER DEN SYSTEMSTATUS ERSTELLEN

Damit die Support-Spezialisten von Kaspersky Lab Sie bei der Lösung eines Problems unterstützen können, kann es erforderlich sein, einen Bericht über den Zustand des Systems zu erstellen. Dieser Bericht enthält ausführliche Informationen über gestartete Prozesse, geladene Module und Treiber, Erweiterungsmodule für Microsoft Internet Explorer und Microsoft Windows Explorer, offene Ports, gefundene verdächtige Objekte u.a.

Beim Erstellen des Berichts über den Systemzustand werden keine persönlichen Benutzerdaten gesammelt.

Gehen Sie folgendermaßen vor, um einen Bericht über den Systemzustand zu erstellen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Bereich des Programmfensters auf den Link **Support**.
3. Klicken Sie im folgenden Fenster **Support** auf den Link **Protokollierung**.
4. Klicken Sie im folgenden Fenster **Informationen für den Support** auf **Bericht über den Systemstatus erstellen**.

Der Bericht über den Systemzustand wird in den Formaten html und xml erstellt und im Archiv sysinfo.zip gespeichert. Nachdem das Sammeln von Daten über das System abgeschlossen wurde, können Sie einen Bericht ansehen.

Gehen Sie folgendermaßen vor, um einen Bericht anzuzeigen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Bereich des Programmfensters auf den Link **Support**.
3. Klicken Sie im folgenden Fenster **Support** auf den Link **Protokollierung**.
4. Klicken Sie im folgenden Fenster **Informationen für den Support** auf **Anzeigen**.
5. Öffnen Sie das Archiv sysinfo.zip, das die Protokolldateien enthält.

PROTOKOLLDATEI ERSTELLEN

Nach der Installation von Kaspersky PURE können bei der Arbeit des Betriebssystems oder bestimmter Programme Störungen auftreten. Dies deutet höchstwahrscheinlich auf einen Konflikt von Kaspersky PURE mit einem Programm, das auf Ihrem Computer installiert ist, oder mit auf Ihrem Computer vorhandenen Treibern hin. Damit die Support-Spezialisten von Kaspersky Lab Sie bei der Lösung Ihres Problems unterstützen können, kann es sein, dass der Support Sie auffordert, eine Protokolldatei zu erstellen.

Gehen Sie folgendermaßen vor, um eine Protokolldatei zu erstellen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Bereich des Programmfensters auf den Link **Support**.
3. Klicken Sie im folgenden Fenster **Support** auf den Link **Protokollierung**.
4. Wählen Sie im folgenden Fenster **Informationen für den Support** unter **Protokollierung** aus der Dropdown-Liste ein Protokollierungsniveau.

   Es wird empfohlen, die Support-Experten nach dem erforderlichen Tracing-Niveau zu fragen. Sollte diese Angabe des Supports fehlen, dann empfohlen, das Tracing-Niveau **500** einzustellen.
5. Klicken Sie auf **Aktivieren**, um den Protokollierungsvorgang zu starten.
6. Wiederholen Sie die Situation, in der das Problem aufgetreten ist.
7. Klicken Sie auf **Deaktivieren**, um den Protokollierungsvorgang zu beenden.

Sie können mit dem Hochladen der Protokollierungsergebnisse (s. Abschnitt "Datendateien versenden" auf S. 253) auf den Server von Kaspersky Lab beginnen.

DATEIEN MIT DATEN SENDEN

Nachdem die Protokolldateien und der Bericht über den Systemzustand erstellt wurden, müssen diese an den Technischen Support von Kaspersky Lab geschickt werden.

Um die Dateien mit den Daten auf den Server des Technischen Supports hochzuladen, benötigen Sie eine Anfragenummer. Diese Nummer erhalten Sie in Ihrem Kaspersky Account auf der Webseite des Technischen Supports, wenn eine aktive Anfrage vorliegt.

Gehen Sie folgendermaßen vor, um die Dateien mit den Daten auf den Server des Technischen Supports hochzuladen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Bereich des Programmfensters auf den Link **Support**.

3. Klicken Sie im folgenden Fenster **Support** auf den Link **Protokollierung**.

4. Klicken Sie im folgenden Fenster **Informationen für den Support** im Block **Aktionen** auf **Informationen für den Support auf den Server laden**.

5. Aktivieren Sie im folgenden Fenster **Support-Informationen auf Server hochladen** die Kontrollkästchen für die Dateien, die Sie an den Technischen Support schicken möchten, und klicken Sie auf **Senden**.

6. Geben Sie im folgenden Fenster **Anfragenummer** die Nummer an, die Ihre Anfrage beim Ausfüllen des Online-Formulars auf der Webseite des Technischen Supports erhalten hat.

Die gewählten Dateien werden komprimiert und an den Server des Technischen Supports gesendet.

Falls kein Kontakt mit dem Technischen Support möglich ist, können Sie diese Dateien auf Ihrem Computer speichern und sie später aus Mein Kaspersky Account absenden.

Gehen Sie folgendermaßen vor, um die Dateien mit Daten auf der Festplatte zu speichern:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im unteren Bereich des Programmfensters auf den Link **Support**.

3. Klicken Sie im folgenden Fenster **Support** auf den Link **Protokollierung**.

4. Klicken Sie im folgenden Fenster **Informationen für den Support** im Block **Aktionen** auf **Informationen für den Support auf den Server laden**.

5. Aktivieren Sie im folgenden Fenster **Support-Informationen auf Server hochladen** die Kontrollkästchen für die Dateien, die Sie an den Technischen Support schicken möchten, und klicken Sie auf **Senden**.

6. Klicken Sie im folgenden Fenster **Anfragenummer** auf **Abbrechen** und bestätigen Sie im folgenden Fenster mit **Ja**, dass die Dateien auf der Festplatte gespeichert werden sollen.

7. Geben Sie im folgenden Fenster einen Namen für das Archiv an und bestätigen Sie das Speichern.

Das fertige Archiv können Sie über Mein Kaspersky Account an den Technischen Support senden.

AVZ-SKRIPT AUSFÜHREN

Die Spezialisten von Kaspersky Lab analysieren Ihr Problem auf der Grundlage von Protokolldateien und eines Berichts über den Systemzustand. Das Ergebnis der Analyse besteht aus einer Reihe von Aktionen, die dazu dienen, die gefundenen Probleme zu beheben. Oft handelt es sich dabei um sehr viele Aktionen.

Um die Problembehebung zu vereinfachen, werden AVZ-Skripts verwendet. Ein AVZ-Skript ist eine Kombination von Befehlen, die es erlauben, Registrierungsschlüssel zu ändern, Dateien in die Quarantäne zu verschieben, eine Klassensuche mit der Möglichkeit der Isolierung von damit verbundenen Dateien vorzunehmen, Hooks der Typen UserMode und KernelMode zu blockieren, u.a.

Zum Starten der Skripts bietet das Programm einen *Assistenten zum Ausführen von AVZ-Skripts*.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**. Zum Abschluss des Assistenten dient die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf **Abbrechen** abgebrochen werden.

Es wird davor gewarnt, den Text eines Skripts, das Ihnen von den Support-Spezialisten geschickt wurde, zu verändern. Sollten bei der Skript-Ausführung Probleme auftreten, dann wenden Sie sich an den Technischen Support.

Gehen Sie folgendermaßen vor, den Assistenten zu starten:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im unteren Bereich des Programmfensters auf den Link **Support**.

3. Klicken Sie im folgenden Fenster **Support** auf den Link **Protokollierung**.

4. Klicken Sie im folgenden Fenster **Informationen für den Support** auf **AVZ-Skript ausführen**.

Wenn das Skript erfolgreich ausgeführt wurde, wird die der Assistent abgeschlossen. Falls bei der Skript-Ausführung Störungen auftreten, zeigt der Assistent eine entsprechende Meldung an.

ANHÄNGE

Dieser Abschnitt enthält Hilfeinformationen, die den Haupttext des Dokuments ergänzen.

IN DIESEM ABSCHNITT

Varianten für den Abo-Status 256

Bedienung des Programms über die Befehlszeile 257

Liste der Benachrichtigungen von Kaspersky PURE 267

VARIANTEN FÜR DEN ABO-STATUS

Es bestehen folgende Varianten für den Abonnementstatus:

- *wird ermittelt*. Die Anfrage auf Aktivierung des Abonnements wurde noch nicht verarbeitet (für die Verarbeitung der Anfrage wird auf dem Server eine bestimmte Zeit benötigt). Kaspersky PURE arbeitet im vollfunktionalen Modus. Wenn die Abonnementanfrage nach Ablauf eines bestimmten Zeitraums nicht verarbeitet wurde, werden Sie darüber benachrichtigt, dass der Abonnementstatus nicht aktualisiert ist. Gleichzeitig werden die Programm-Datenbanken nicht mehr aktualisiert (für eine Lizenz mit Update-Abonnement) und der Computerschutz wird beendet (für eine Lizenz mit Update- und Schutz-Abonnement).

- *wurde aktiviert*. Das Abonnement wurde unbegrenzt oder für einen bestimmten Zeitraum aktiviert (festes Ablaufdatum des Abonnements).

- *wurde verlängert*. Das Abonnement wurde unbegrenzt oder für einen bestimmten Zeitraum verlängert.

- *Fehler*. Bei Aktualisierung des Abonnementstatus ist ein Fehler aufgetreten.

- *ist abgelaufen. Ihnen wird eine Ermässigung gewährt.* Die Gültigkeit des Abonnements oder der Zeitraum, während dem der Abonnementstatus aktualisiert werden muss, ist abgelaufen. Wenn der Zeitraum, während dem der Abonnementstatus aktualisiert werden muss, abgelaufen ist, aktualisieren Sie den Abonnementstatus manuell. Wenn die Gültigkeit des Abonnements abgelaufen ist, können Sie das Abonnement verlängern. Wenden Sie sich dazu an den Online-Shop, bei dem Sie Kaspersky PURE erworben haben. Um einen anderen Aktivierungscode zu verwenden, muss das verwendete Abonnement zuerst gelöscht werden.

- *ist abgelaufen. Die Ermässigungsfrist ist abgelaufen.* Die Gültigkeit des Abonnements oder die Ermäßigungsfrist für Lizenzverlängerung ist abgelaufen. Wenden Sie sich an den Lieferanten des Abonnements, um ein neues Abonnement zu kaufen oder das vorhandene Abonnement zu aktualisieren.

  Wenn die Gültigkeit des Abonnements abgelaufen und die Ermäßigungsfrist, in der eine Verlängerung möglich war, verstrichen ist (Abo-Status – *Abgelaufen*), benachrichtigt Kaspersky PURE Sie darüber und versucht nicht mehr, das Abonnement automatisch zu verlängern. Für eine Lizenz mit Update-Abonnement bleibt die Funktionalität des Programms unter Ausnahme des Updates der Programm-Datenbanken erhalten. Für eine Lizenz mit Update- und Schutz-Abonnement werden die Datenbanken des Programms nicht mehr aktualisiert, der Computerschutz wird eingestellt und die Untersuchungsaufgaben werden nicht mehr gestartet.

- *Das Abonnement wurde gekündigt*. Sie haben die Verwendung eines Abonnements zur automatischen Lizenzverlängerung verworfen.

- *Aktualisierung ist erforderlich*. Der Abonnementstatus wurde aus bestimmten Gründen nicht rechtzeitig aktualisiert.

  Wenn das Abonnement nicht rechtzeitig aktualisiert wurde (wenn beispielsweise der Computer während des gesamten Zeitraums ausgeschaltet war, in dem eine Lizenzverlängerung möglich war), können Sie den Abo-

Status im Fenster Lizenzverwaltung manuell aktualisieren (s. Abschnitt "Lizenz-Info anzeigen" auf S. 43). Bis zur Verlängerung des Abonnements lädt Kaspersky PURE keine Updates für die Programm-Datenbanken herunter (für eine Lizenz mit Update-Abonnement), stellt den Computerschutz ein und startet keine Untersuchungsaufgaben (für eine Lizenz mit Update- und Schutz-Abonnement).

- *wurde angehalten*. Abonnement zur automatischen Lizenzverlängerung wurde angehalten.
- *wurde erneuert*. Das Abonnement wurde aktualisiert.

In einigen Fällen können für eine Lizenz mit Abonnement zusätzliche Informationen zum Abo-Status angezeigt werden.

BEDIENUNG DES PROGRAMMS ÜBER DIE BEFEHLSZEILE

Sie können Kaspersky PURE mit Hilfe der Befehlszeile steuern. Dabei ist die Möglichkeit zum Ausführen der folgenden Operationen vorgesehen:

- Programm aktivieren
- Programm starten und beenden
- Programmkomponenten starten und beenden.
- Aufgaben starten und beenden
- Erhalt von Informationen über den aktuellen Status von Komponenten und Aufgaben und ihrer Statistik.
- Ausführung von Untersuchungsaufgaben starten und beenden.
- Untersuchung von ausgewählten Objekten.
- Update der Datenbanken und Programm-Module, Rollback von Updates.
- Export und Import von Schutzparametern.
- Aufruf der Hilfe über die Syntax der Befehlszeile insgesamt und für einzelne Befehle.

Syntax der Befehlszeile:

```
avp.com <Befehl> [Parameter]
```

Der Zugriff auf das Programm über die Befehlszeile muss aus dem Installationsordner des Produkts oder unter Angabe des vollständigen Pfads von avp.com erfolgen.

Die Liste der Befehle, die für die Steuerung des Programms und seiner Komponenten verwendet werden, finden Sie in der nachstehenden Tabelle.

START	Komponente oder Aufgabe starten
STOP	Beenden der Arbeit einer Komponente oder Aufgabe (die Ausführung des Befehls ist nur möglich, wenn das Kennwort eingegeben wird, das auf dem Interface von Kaspersky PURE festgelegt wurde)
STATUS	Bildschirmanzeige des aktuellen Status einer Komponente oder Aufgabe
STATISTICS	Bildschirmanzeige der Statistik über die Arbeit einer Komponente oder Aufgabe
HELP	Anzeige der Befehlsliste sowie von Informationen über die Befehlssyntax auf dem Bildschirm

SCAN	Untersuchung von Objekten auf das Vorhandensein von Viren
UPDATE	Programm-Update starten
ROLLBACK	Rückgängigmachen des zuletzt durchgeführten Updates von Kaspersky PURE (die Ausführung des Befehls ist nur möglich, wenn das Kennwort eingegeben wird, das über die Programmoberfläche festgelegt wurde)
EXIT	Beenden der Arbeit mit dem Programm (dieser Befehl kann nur ausgeführt werden, wenn das über die Programmoberfläche festgelegte Kennwort angegeben wird)
IMPORT	Importieren von Schutzeinstellungen für Kaspersky PURE (die Ausführung des Befehls ist nur möglich, wenn über die Programmoberfläche festgelegte Kennwort angegeben wird)
EXPORT	Schutzparameter des Programms exportieren

Jedem Befehl entspricht eine eigene Auswahl von Parametern, die für eine konkrete Komponente des Programms spezifisch sind.

IN DIESEM ABSCHNITT

Programm aktivieren 258

Programm starten 259

Programm beenden 259

Steuerung von Komponenten und Aufgaben des Programms 259

Virensuche 261

Programm-Update 263

Rollback zum vorherigen Update 264

Schutzparameter exportieren 264

Schutzparameter importieren 265

Protokolldatei anlegen 265

Hilfe anzeigen 266

Rückgabecodes der Befehlszeile 266

PROGRAMM AKTIVIEREN

Kaspersky PURE kann mit Hilfe einer Schlüseldatei aktiviert werden.

Befehlssyntax:

```
avp.com ADDKEY <Dateiname>
```

Eine Beschreibung der Parameter für die Befehlsausführung ist in der nachstehenden Tabelle zu finden.

<Dateiname>	Name der Lizenzschlüsseldatei für das Programm (Endung .key).

Beispiel:

```
avp.com ADDKEY 1AA111A1.key
```

PROGRAMM STARTEN

Befehlssyntax:

```
avp.com
```

PROGRAMM BEENDEN

Befehlssyntax:

```
avp.com EXIT /password=<Kennwort>
```

Folgende Tabelle beschreibt die Parameter.

<Kennwort>	Kennwort für das Programm, das über die Programmoberfläche festgelegt wurde.

Beachten Sie, dass dieser Befehl nicht ausgeführt wird, wenn das Kennwort nicht eingegeben wird.

STEUERUNG VON KOMPONENTEN UND AUFGABEN DES PROGRAMMS

Befehlssyntax:

```
avp.com <Befehl> <Profil|Aufgabenname> [/R[A]:<Berichtsdatei>]
avp.com STOP <Profil|Aufgabenname> /password=<Kennwort> [/R[A]:<Berichtsdatei>]
```

Befehle und Parameter werden in folgender Tabelle beschrieben.

<Befehl>	Die Steuerung der Komponenten und Aufgaben von Kaspersky PURE wird mit Hilfe der folgenden Befehle ausgeführt: START – Start einer Schutzkomponente oder einer Aufgabe. STOP – Beenden einer Schutzkomponente oder einer Aufgabe. STATUS – Aktuellen Status einer Komponente oder Aufgabe auf dem Bildschirm anzeigen. STATISTICS – Die Statistik über die Arbeit einer Schutzkomponente oder einer Aufgabe auf dem Bildschirm anzeigen. Beachten Sie, dass der Befehl STOP nur ausgeführt wird, wenn das Kennwort eingegeben wird.
<Profil|Aufgabenname>	Als Wert für den Parameter **<Profil>** sind möglich: eine beliebige Schutzkomponente von Kaspersky PURE, Module, die zu den Komponenten gehören, erstellte Untersuchungs- oder Updateaufgaben (die vom Programm standardmäßig verwendeten Werte werden in folgender Tabelle genannt). Als Wert für den Parameter **<Aufgabenname>** kann der Name einer beliebigen vom Benutzer erstellten Untersuchungs- oder Updateaufgabe angegeben werden.

<Kennwort>	Kennwort für das Programm, das über die Programmoberfläche festgelegt wurde.
/R[A]:<Berichtsdatei>	**/R:<Berichtsdatei>** – nur wichtige Ereignisse im Bericht protokollieren. **/RA:<Berichtsdatei>** - alle Ereignisse im Bericht protokollieren. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.

Für den Parameter **<Profil>** wird einer der Werte aus folgender Tabelle angegeben.

RTP	Alle Schutzkomponenten. Der Befehl **avp.com START RTP** startet alle Schutzkomponenten, wenn der Schutz vollständig deaktiviert war. Wenn eine Komponente mit dem Befehl **STOP** aus der Befehlszeile beendet wurde, wird sie durch den Befehl **avp.com START RTP** nicht gestartet. Um die Komponente zu starten, ist der Befehl **avp.com START <Profil>** erforderlich, wobei als **<Profil>** der Wert der betreffenden Schutzkomponente verwendet wird, beispielsweise **avp.com START FM**.
FW	Firewall.
HIPS	Programmkontrolle.
pdm	Proaktiver Schutz.
FM	Datei-Anti-Virus.
EM	Mail-Anti-Virus.
WM	Web-Anti-Virus. Werte für die Subkomponenten von Web-Anti-Virus: **httpscan (HTTP)** – Untersuchung des http-Datenstroms **sc** – Skript-Untersuchung
IM	IM-Anti-Virus.
AB	Anti-Banner
AS	Anti-Spam.
PC	Kindersicherung.
AP	Anti-Phishing.
ids	Schutz vor Netzwerkangriffen.
Updater	Update.
Rollback	Rollback zum vorherigen Update.
Scan_My_Computer	Untersuchung des Computers.
Scan_Objects	Objekte untersuchen.
Scan_Quarantine	Quarantäne untersuchen.

Scan_Startup (STARTUP)	Autostart-Objekte untersuchen.
Scan_Vulnerabilities (SECURITY)	Schwachstellensuche.

Die aus der Befehlszeile gestarteten Komponenten und Aufgaben werden mit den Parametern ausgeführt, die über die Programmoberfläche festgelegt wurden.

Beispiele:

- *Geben Sie folgenden Befehl ein, um Datei-Anti-Virus zu aktivieren:*

```
avp.com START FM
```

- *Geben Sie folgenden Befehl ein, um die Untersuchung des Computers abzubrechen:*

```
avp.com STOP Scan_My_Computer /password=<Kennwort>
```

VIRENSUCHE

Die Befehlszeile zum Starten der Virenuntersuchung eines bestimmten Bereichs und zum Starten der Verarbeitung von schädlichen Objekten besitzt folgendes allgemeines Aussehen:

```
avp.com SCAN [<Untersuchungsobjekt>] [<Aktion>] [<Dateitypen>] [<Ausnahmen>]
[<Konfigurationsdatei>] [<Berichtsparameter>] [<zusätzliche Parameter>]
```

Für die Untersuchung von Objekten können Sie auch die im Programm erstellten Aufgaben verwenden, die aus der Befehlszeile gestartet werden können. Dabei wird die Aufgabe mit den Parametern ausgeführt, die über die Oberfläche von Kaspersky PURE festgelegt wurden.

Folgende Tabelle beschreibt die Parameter.

<Untersuchungsobjekt> – Der Parameter gibt eine Liste der Objekte an, die auf das Vorhandensein von schädlichem Code untersucht werden sollen. Der Parameter kann mehrere Werte aus der folgenden Liste enthalten. Die Werte werden durch Leerzeichen getrennt.	
<files>	Liste mit den Pfaden der Dateien und Ordner für die Untersuchung. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Als Trennzeichen für die Elemente der Liste dient das Leerzeichen. Kommentare: • Wenn der Objektname ein Leerzeichen enthält, wird er in Anführungszeichen gesetzt. • Wenn ein konkreter Ordner angegeben wird, werden alle darin enthaltenen Dateien untersucht.
/MEMORY	Objekte des Arbeitsspeichers.
/STARTUP	Autostart-Objekte**.**
/MAIL	Posteingänge.
/REMDRIVES	Alle Wechseldatenträger.
/FIXDRIVES	Alle lokalen Laufwerke.
/NETDRIVES	Alle Netzlaufwerke.
/QUARANTINE	Objekte in Quarantäne.

/ALL	Vollständige Untersuchung des Computers.
/@:<filelist.lst>	Pfad der Datei mit einer Liste der Objekte und Ordner, die untersucht werden sollen. Für die Datei mit der Liste ist die Angabe des absoluten oder relativen Pfads zulässig. Der Pfad wird ohne Anführungszeichen angegeben, selbst wenn er ein Leerzeichen enthält. Die Datei mit der Liste muss das Textformat besitzen. Jedes Untersuchungsobjekt muss in einer separaten Zeile stehen. Es wird empfohlen, in der Datei die absoluten Pfade der Untersuchungsobjekte anzugeben. Bei Angabe eines relativen Pfads wird der Pfad im Bezug auf die ausführbare Programmdatei angegeben, nicht im Bezug auf die Datei mit der Liste der Untersuchungsobjekte.
<Aktion> – Der Parameter bestimmt die Aktionen mit einem schädlichen Objekt, das während der Untersuchung gefunden wird. Wenn der Parameter nicht angegeben wird, wird standardmäßig die Aktion ausgeführt, die dem Wert **/i8** entspricht. Wenn Sie im automatischen Modus arbeiten, wendet Kaspersky PURE beim Fund gefährlicher Objekte automatisch die von Kaspersky Lab empfohlene Aktion an. Die Aktion ausgeführt, die dem **<Aktion>** entspricht, wird ignoriert.	
/i0	Keine Aktion ausführen, Informationen im Bericht protokollieren.
/i1	Infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – überspringen**.**
/i2	Infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – löschen; infizierte Objekte aus Containern (zusammengesetzten Objekten) nicht löschen; Container mit ausführbarer Kopfzeile (sfx-Archive) löschen.
/i3	infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – löschen; Container-Objekte vollständig löschen, wenn die darin enthaltenen infizierten Dateien nicht gelöscht werden können.
/i4	infizierte Objekte löschen; Container-Objekte vollständig löschen, wenn die darin enthaltenen infizierten Dateien nicht gelöscht werden können.
/i8	Beim Fund eines infizierten Objekts den Benutzer nach der Aktion fragen.
/i9	Den Benutzer nach der Aktion fragen, wenn die Untersuchung abgeschlossen wird.
<Dateitypen> – Der Parameter bestimmt die Typen der Dateien, die der Virenuntersuchung unterzogen werden. Wenn der Parameter nicht angegeben wird, werden standardmäßig nur infizierbare Dateien nach ihrem Inhalt untersucht.	
/fe	Nur infizierbare Dateien nach Erweiterung untersuchen.
/fi	Nur infizierbare Dateien nach Inhalt untersuchen.
/fa	**Alle Dateien untersuchen**.
<Ausnahmen> – Der Parameter bestimmt die Objekte, die von der Untersuchung ausgeschlossen werden sollen. Der Parameter kann mehrere Werte aus der folgenden Liste enthalten. Die Werte werden durch Leerzeichen getrennt.	
-e:a	Archive nicht untersuchen.
-e:b	Mail-Datenbanken nicht untersuchen.
-e:m	E-Mail-Nachrichten im Format plain text nicht untersuchen.
-e:<filemask>	Objekte nach Maske nicht untersuchen.

-e:<seconds>	Objekte überspringen, deren Untersuchung länger dauert, als der durch den Parameter **<seconds>** angegebene Zeitraum.
-es:<size>	Objekte überspringen, deren Größe (in MB) über dem Wert liegt, der durch den Parameter **<size>** angegeben wird. Der Parameter ist nur auf zusammengesetzte Dateie (z.B. Archive) anwendbar.
<Konfigurationsdatei> – bestimmt den Pfad der Konfigurationsdatei, in der die Parameter für die Arbeit des Programms bei der Untersuchung enthalten sind. Die Konfigurationsdatei ist eine Datei im Textformat, die eine Auswahl von Befehlszeilenparametern für die Antiviren-Untersuchung enthält. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Werte verwendet, die über die Programmoberfläche festgelegt wurden.	
/C:<Dateiname>	Die Werte der Parameter, die in der Datei **<Dateiname>** angegeben sind, verwenden.
<Berichtsparameter> – Der Parameter bestimmt das Format des Berichts über die Untersuchungsergebnisse. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.	
/R:<Berichtsdatei>	Nur wichtige Ereignisse in der angegebenen Berichtsdatei protokollieren.
/RA:<Berichtsdatei>	Alle wichtigen Ereignisse in der angegebenen Berichtsdatei protokollieren.
<zusätzliche Parameter> – Parameter, der die Verwendung von Technologien zur Virenuntersuchung festlegt.	
/iChecker=<on|off>	Verwendung der Technologie iChecker aktivieren / deaktivieren.
/iSwift=<on|off>	Verwendung der Technologie iSwift aktivieren / deaktivieren.

Beispiele:

- *Untersuchung des Arbeitsspeichers, der Autostart-Objekte, der Mailboxen sowie der Ordner Eigene Dateien, Programme und der Datei test.exe:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My
Documents" "C:\Program Files" "C:\Downloads\test.exe"
```

- *Untersuchung der Objekte, deren Liste in der Datei object2scan.txt angegeben ist. Für die Arbeit soll die Konfigurationsdatei scan_settings.txt verwendet werden. Über die Untersuchungsergebnisse soll ein Bericht erstellt werden, in dem alle Ereignisse aufgezeichnet werden:*

```
avp.com SCAN /MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

Beispiel für die Konfigurationsdatei:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

PROGRAMM-UPDATE

Der Befehl für das Update der Programm-Module und Datenbanken von Kaspersky PURE besitzt folgende Syntax:

```
avp.com UPDATE [<Updatequelle>] [/R[A]:<Berichtsdatei>] [/C:<Dateiname>]
```

Folgende Tabelle beschreibt die Parameter.

<Updatequelle>	HTTP-, FTP-Server oder Netzwerkordner für den Download von Updates. Als Wert für diesen Parameter kann der vollständige Pfad oder die URL-Adresse der Updatequelle angegeben werden. Wenn der Pfad nicht angegeben wird, wird die Updatequelle aus den Parametern des Diensts für das Programm-Update übernommen.
/R[A]:<Berichtsdatei>	**/R:**<Berichtsdatei> – nur wichtige Ereignisse im Bericht protokollieren.

	/RA:<Berichtsdatei> - alle Ereignisse im Bericht protokollieren. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.
/C:<Dateiname>	Pfad der Konfigurationsdatei, die die Parameter für die Arbeit von Kaspersky PURE beim Update enthält. Die Konfigurationsdatei ist eine Textdatei, die eine Auswahl von Befehlszeilenparametern für das Update des Programms enthält. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Werte verwendet, die über die Programmoberfläche festgelegt wurden.

Beispiele:

- *Update der Programm-Datenbanken, alle Ereignisse im Bericht protokollieren:*

```
avp.com UPDATE /RA:avbases_upd.txt
```

- *Update der Programm-Module von Kaspersky PURE, die Parameter der Konfigurationsdatei updateapp.ini verwenden:*

```
avp.com UPDATE /C:updateapp.ini
```

Beispiel für die Konfigurationsdatei:

```
"ftp://my_server/kav updates" /RA:avbases_upd.txt
```

ROLLBACK ZUM VORHERIGEN UPDATE

Befehlssyntax:

```
avp.com ROLLBACK [/R[A]:<Berichtsdatei>][/password=<Kennwort>]
```

Folgende Tabelle beschreibt die Parameter.

/R[A]:<Berichtsdatei>	**/R:**<Berichtsdatei> – nur wichtige Ereignisse im Bericht protokollieren. **/RA:**<Berichtsdatei> - alle Ereignisse im Bericht protokollieren. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.
<Kennwort>	Kennwort für das Programm, das über die Programmoberfläche festgelegt wurde.

Beachten Sie, dass dieser Befehl nicht ausgeführt wird, wenn das Kennwort nicht eingegeben wird.

Beispiel:

```
avp.com ROLLBACK /RA:rollback.txt /password=<Kennwort>
```

SCHUTZPARAMETER EXPORTIEREN

Befehlssyntax:

```
avp.com EXPORT <Profil> <Dateiname>
```

Eine Beschreibung der Parameter für die Befehlsausführung ist in der nachstehenden Tabelle zu finden.

<Profil>	Komponente oder Aufgabe, für die der Export von Parametern ausgeführt wird. Als Wert des Parameters **<Profil>** kann ein beliebiger Wert dienen, der im Hilfeabschnitt "Steuerung von Komponenten und Aufgaben des Programms" genannt wird.
<Dateiname>	Pfad der Datei, in welche die Parameter von Kaspersky PURE exportiert werden. Ein absoluter oder relativer Pfad kann angegeben werden. Die Konfigurationsdatei wird im Binärformat (dat) gespeichert und kann künftig verwendet werden, um die Einstellungen des Programms auf andere Computer zu übertragen. Außerdem können Sie die Konfigurationsdatei im Textformat speichern. Geben Sie dazu im Dateinamen die Endung txt an. Beachten Sie, dass der Import von Schutzparametern aus einer Textdatei nicht unterstützt wird. Diese Datei kann nur zur Ansicht der grundlegenden Funktionsparameter von Kaspersky PURE verwendet werden.

Beispiel:

```
avp.com EXPORT RTP c:\settings.dat
```

SCHUTZPARAMETER IMPORTIEREN

Befehlssyntax:

```
avp.com IMPORT <Dateiname> [/password=<Kennwort>]
```

Eine Beschreibung der Parameter für die Befehlsausführung ist in der nachstehenden Tabelle zu finden.

<Dateiname>	Pfad der Datei, aus welcher die Parameter von Kaspersky PURE importiert werden. Ein absoluter oder relativer Pfad kann angegeben werden.
<Kennwort>	Kennwort für Kaspersky PURE, das über die Programmoberfläche festgelegt wurde. <Kennwort>

Beachten Sie, dass dieser Befehl nicht ausgeführt wird, wenn das Kennwort nicht eingegeben wird.

Beispiel:

```
avp.com IMPORT c:\settings.dat /password=<Ihr_Kennwort>
```

PROTOKOLLDATEI ANLEGEN

Das Anlegen einer Protokolldatei kann erforderlich sein, wenn bei der Arbeit von Kaspersky PURE Probleme auftreten. Die Protokolldatei ermöglicht den Experten des Technischen Supports eine genaue Problemanalyse.

Es wird empfohlen, das Anlegen von Tracing-Dateien nur zur Diagnose eines konkreten Problems zu aktivieren. Sollte das Tracing ständig aktiv sein, so kann die Leistungsfähigkeit des Computers sinken und es kann zur Überfüllung der Festplatte kommen.

Befehlssyntax:

```
avp.com TRACE [file] [on|off] [<Tracing-Niveau>]
```

Folgende Tabelle beschreibt die Parameter.

[on|off]	Anlegen einer Protokolldatei aktivieren / deaktivieren.
[file]	Tracing in Form einer Datei erstellen.
<Tracing-Niveau>	Für diesen Parameter kann ein Zahlenwert im Bereich von 0 (minimale Stufe, nur kritische Meldungen) bis 700 (maximale Stufe, alle Meldungen) festgelegt werden. Wenn Sie sich an den Technischen Support wenden, nennt Ihnen der zuständige Spezialist das erforderliche Tracing-Niveau. Andernfalls gilt das Niveau 500 als empfehlenswert.

Beispiele:

- *Erstellen von Protokolldateien deaktivieren:*

  ```
  avp.com TRACE file off
  ```

- *Erstellen einer Tracing-Datei zum Senden an den Technischen Support, mit einem maximalen Tracing-Niveau von 500:*

  ```
  avp.com TRACE file on 500
  ```

HILFE ANZEIGEN

Folgender Befehl dient zur Anzeige von Hilfeinformationen über die Syntax der Befehlzeile:

```
avp.com [ /? | HELP ]
```

Um Hilfeinformationen über die Syntax eines konkreten Befehls zu erhalten, können Sie einen der folgenden Befehle verwenden:

```
avp.com <Befehl> /?
avp.com HELP <Befehl>
```

RÜCKGABECODES DER BEFEHLSZEILE

In diesem Abschnitt werden die Rückgabecodes der Befehlszeile beschrieben (s. folgende Tabelle). Die allgemeinen Codes können von einem beliebigen Befehl der Befehlszeile zurückgegeben werden. Als Rückgabecodes für Aufgaben sind die allgemeinen Codes sowie spezifische Codes für einen konkreten Aufgabentyp möglich.

ALLGEMEINE RÜCKGABECODES	
0	Operation wurde erfolgreich ausgeführt
1	Ungültiger Parameterwert
2	Unbekannter Fehler
3	Fehler bei Ausgabenausführung
4	Aufgabenausführung wurde abgebrochen
RÜCKGABECODES FÜR AUFGABEN ZUR VIRENSUCHE	
101	Alle gefährlichen Objekte wurden bearbeitet
102	Es wurden gefährliche Objekte gefunden

LISTE DER BENACHRICHTIGUNGEN VON KASPERSKY PURE

Dieser Abschnitt bietet eine Liste der Benachrichtigungen, die bei der Arbeit von Kaspersky PURE auf dem Bildschirm erscheinen können.

IN DIESEM ABSCHNITT

Desinfektion des Objekts ist nicht möglich 267

Nicht verfügbarer Updateserver 268

Verdächtiges Objekt wurde gefunden 268

Gefährliches Objekt wurde im Datenstrom gefunden 269

Verdächtiges Objekt wurde gefunden 269

Gefährliche Aktivität im System wurde erkannt 270

Versteckter Prozess wurde gefunden 271

Versuch zum Zugriff auf die Systemregistrierung wurde erkannt 271

Netzwerkaktivität eines Programms wurde erkannt 272

Neues Netzwerk wurde gefunden 273

Phishing-Angriff wurde erkannt 273

Verdächtiger Link wurde gefunden 273

Ein inkorrektes Zertifikat wurde gefunden 274

Zeitbeschränkung für die Verwendung eines Programms 274

Spezielle Desinfektionsprozedur ist erforderlich 274

Die Datei ist bereits vorhanden 274

DESINFEKTION DES OBJEKTS IST NICHT MÖGLICH

In bestimmten Fällen ist die Desinfektion eines schädlichen Objekts nicht möglich. So kann eine Datei beispielsweise so stark beschädigt sein, dass es nicht möglich ist, den schädlichen Code daraus zu löschen und sie vollständig wiederherzustellen. Außerdem ist die Desinfektionsprozedur nicht einige Arten von schädlichen Objekten wie z.B. Trojaner-Programme nicht anwendbar.

In solchen Fällen erscheint auf dem Bildschirm eine spezielle Meldung, die folgende Informationen enthält:

- Art der Bedrohung (beispielsweise *Virus*, *trojanisches Programm*) und Name des schädlichen Objekts, der seiner Bezeichnung in der Viren-Enzyklopädie von Kaspersky Lab entspricht. Der Name des schädlichen Objekts besitzt die Form eines Links zu der Ressource http://www.viruslist.com/de, auf der Sie ausführliche Informationen darüber erhalten können, welche Art von Bedrohung auf Ihrem Computer gefunden wurde.

- Vollständiger Name und Pfad des schädlichen Objekts.

Ihnen wird angeboten, eine der folgenden Aktionen für das Objekt auszuwählen:

- **Löschen** – Das schädliche Objekt löschen. Vor dem Löschen wird eine Sicherungskopie des Objekts angelegt, um bei Bedarf das Objekt oder ein Infektionsbild wiederherstellen zu können.

- **Überspringen** - Der Zugriff auf das Objekt wird gesperrt. Keine Aktion mit dem Objekt vornehmen, sondern nur Informationen darüber im Bericht aufzeichnen.

  Sie können später aus dem Berichtsfenster zur Verarbeitung von übersprungenen schädlichen Objekten zurückkehren (für Objekte, die in E-Mails gefunden wurden, steht die Option zur aufgeschobenen Verarbeitung nicht zur Verfügung).

Damit die ausgewählte Aktion auf alle Objekte mit dem gleichen Status angewendet wird, die während der laufenden Sitzung der Schutzkomponente oder Aufgabe gefunden werden, aktivieren Sie das Kontrollkästchen ☑ **In allen ähnlichen Fällen anwenden**. Als laufende Sitzung gelten die Arbeitszeit einer Komponente ab dem Zeitpunkt ihres Starts bis zum Moment des Ausschaltens oder Neustarts des Programms, sowie die Ausführungszeit einer Untersuchungsaufgabe ab dem Start bis zum Abschluss.

NICHT VERFÜGBARER UPDATESERVER

Wenn ein momentan nicht verfügbarer Computer, der für einen oder mehrere Computer eines Netzwerks als Updateserver dient, ist eine rechtzeitige Aktualisierung von Kaspersky PURE nicht möglich. In diesem Fall ist die Sicherheit des Netzwerks gefährdet und Kaspersky PURE protokolliert das Ereignis im Statusbericht des Netzwerkschutzes.

Aus Sicherheitsgründen muss entweder der nicht verfügbare Computer eingeschaltet oder ein anderer Computer als Updatequelle definiert werden.

VERDÄCHTIGES OBJEKT WURDE GEFUNDEN

Wenn von Datei-Anti-Virus, Mail-Anti-Virus oder von einer Untersuchungsaufgabe ein schädliches Objekt gefunden wird, erscheint eine spezielle Meldung auf dem Bildschirm.

Sie enthält:

- Art der Bedrohung (beispielsweise *Virus*, *trojanisches Programm*) und Name des schädlichen Objekts, der seiner Bezeichnung in der Viren-Enzyklopädie von Kaspersky Lab entspricht. Der Name des schädlichen Objekts besitzt die Form eines Links zu der Ressource http://www.viruslist.com/de, auf der Sie ausführliche Informationen darüber erhalten können, welche Art von Bedrohung auf Ihrem Computer gefunden wurde.

- Vollständiger Name und Pfad des schädlichen Objekts.

Ihnen wird angeboten, eine der folgenden Aktionen für das Objekt auszuwählen:

- **Desinfizieren** – Es wird versucht, das schädliche Objekt zu desinfizieren. Vor der Desinfektion wird eine Sicherungskopie des Objekts angelegt, um bei Bedarf das Objekt oder ein Infektionsbild wiederherstellen zu können.

- **Löschen** – Das schädliche Objekt löschen. Vor dem Löschen wird eine Sicherungskopie des Objekts angelegt, um bei Bedarf das Objekt oder ein Infektionsbild wiederherstellen zu können.

- **Überspringen** - Der Zugriff auf das Objekt wird gesperrt. Keine Aktion mit dem Objekt vornehmen, sondern nur Informationen darüber im Bericht aufzeichnen.

  Sie können später aus dem Berichtsfenster zur Verarbeitung von übersprungenen schädlichen Objekten zurückkehren (für Objekte, die in E-Mails gefunden wurden, steht die Option zur aufgeschobenen Verarbeitung nicht zur Verfügung).

Damit die ausgewählte Aktion auf alle Objekte mit dem gleichen Status angewendet wird, die während der laufenden Sitzung der Schutzkomponente oder Aufgabe gefunden werden, aktivieren Sie das Kontrollkästchen ☑ **In allen**

ähnlichen Fällen anwenden. Als laufende Sitzung gilt die Arbeitszeit einer Komponente ab dem Zeitpunkt ihres Starts bis zum Moment des Abschaltens oder Neustarts des Programms, sowie die Ausführungszeit einer Untersuchungsaufgabe ab dem Start bis zum Abschluss.

GEFÄHRLICHES OBJEKT WURDE IM DATENSTROM GEFUNDEN

Wenn Web-Anti-Virus im Datenstrom ein gefährliches Objekt findet, erscheint eine spezielle Meldung auf dem Bildschirm.

Die Meldung enthält:

- Art der Bedrohung (beispielsweise *Virusmodifikation*) und Name des gefährlichen Objekts, der seiner Bezeichnung in der Viren-Enzyklopädie von Kaspersky Lab entspricht. Der Name des Objekts besitzt die Form eines Links zu der Ressource http://www.viruslist.com/de, auf der Sie ausführliche Informationen darüber erhalten können, welche Art von Bedrohung auf Ihrem Computer gefunden wurde.

- Vollständiger Name des gefährlichen Objekts und Pfad der Web-Ressource.

Ihnen wird angeboten, eine der folgenden Aktionen für das Objekt auszuwählen:

- **Erlauben**- Download des Objekts fortsetzen.

- **Verbieten** – Download des Objekts von der Webressource blockieren.

Damit die ausgewählte Aktion auf alle Objekte mit dem gleichen Status angewendet wird, die während der laufenden Sitzung der Schutzkomponente oder Aufgabe gefunden werden, aktivieren Sie das Kontrollkästchen ☑ **In allen ähnlichen Fällen anwenden**. Als laufende Sitzung gilt die Arbeitszeit einer Komponente ab dem Zeitpunkt ihres Starts bis zum Moment des Abschaltens oder Neustarts des Programms, sowie die Ausführungszeit einer Untersuchungsaufgabe ab dem Start bis zum Abschluss.

VERDÄCHTIGES OBJEKT WURDE GEFUNDEN

Wenn von Datei-Anti-Virus, Mail-Anti-Virus oder von einer Untersuchungsaufgabe ein Objekt gefunden wird, das den Code eines unbekannten Virus oder den modifizierten Code eines bekannten Virus enthält, erscheint eine spezielle Meldung auf dem Bildschirm.

Sie enthält:

- Art der Bedrohung (beispielsweise *Virus*, *trojanisches Programm*) und Name des Objekts, der seiner Bezeichnung in der Viren-Enzyklopädie von Kaspersky Lab entspricht. Der Name des schädlichen Objekts besitzt die Form eines Links zu der Ressource http://www.viruslist.com/de, auf der Sie ausführliche Informationen darüber erhalten können, welche Art von Bedrohung auf Ihrem Computer gefunden wurde.

- Vollständiger Name und Pfad des Objekts.

Ihnen wird angeboten, eine der folgenden Aktionen für das Objekt auszuwählen:

- **Quarantäne** - Das Objekt wird in die Quarantäne verschoben. Ein Objekt unter Quarantäne zu stellen, bedeutet, es wird nicht kopiert, sondern verschoben: Das Objekt wird am ursprünglichen Speicherort oder aus einer E-Mail-Nachricht gelöscht und im Quarantäneordner gespeichert. Die unter Quarantäne stehenden Dateien werden in einem speziellen Format gespeichert und stellen keine Gefahr dar.

  Bei späteren Untersuchungen der Quarantäne mit aktualisierten Bedrohungssignaturen kann sich der Status eines Objekts ändern. Das Objekt kann beispielsweise als infiziert erkannt und mit Hilfe aktualisierter Datenbanken verarbeitet werden, oder es erhält den Status *virenfrei* und kann dann wiederhergestellt werden.

Wenn sich eine Datei, die manuell in die Quarantäne verschoben wurde, bei einer späteren Untersuchung als virenfrei erweist, ändert sich ihr Status nicht gleich nach der Untersuchung in *ok*. Der Status ändert sich nur dann sofort, wenn die Untersuchung mindestens drei Tage, nachdem die Datei unter Quarantäne gestellt wurde, stattfindet.

- **Löschen** – Das Objekt löschen. Vor dem Löschen wird eine Sicherungskopie des Objekts angelegt, um bei Bedarf das Objekt oder ein Infektionsbild wiederherstellen zu können.
- **Überspringen** - Der Zugriff auf das Objekt wird gesperrt. Keine Aktion mit dem Objekt vornehmen, sondern nur Informationen darüber im Bericht aufzeichnen.

  Sie können später aus dem Berichtsfenster zur Verarbeitung von übersprungenen schädlichen Objekten zurückkehren (für Objekte, die in E-Mails gefunden wurden, steht die Option zur aufgeschobenen Verarbeitung nicht zur Verfügung).

Damit die ausgewählte Aktion auf alle Objekte mit dem gleichen Status angewendet wird, die während der laufenden Sitzung der Schutzkomponente oder Aufgabe gefunden werden, aktivieren Sie das Kontrollkästchen ☑ **In allen ähnlichen Fällen anwenden**. Als laufende Sitzung gilt die Arbeitszeit einer Komponente ab dem Zeitpunkt ihres Starts bis zum Moment des Abschaltens oder Neustarts des Programms, sowie die Ausführungszeit einer Untersuchungsaufgabe ab dem Start bis zum Abschluss.

Wenn Sie überzeugt sind, dass das gefundene Objekt ungefährlich ist, können Sie es der vertrauenswürdigen Zone hinzufügen, um zu verhindern, dass das Programm bei der Arbeit mit diesem Objekt erneut anspricht.

GEFÄHRLICHE AKTIVITÄT IM SYSTEM WURDE ERKANNT

Wenn der Proaktive Schutz die gefährliche Aktivität einer bestimmten Anwendung im System erkennt, wird auf dem Bildschirm eine spezielle Meldung angezeigt, die folgende Informationen enthält:

- Name der Bedrohung, der ihrer Bezeichnung in der Viren-Enzyklopädie von Kaspersky Lab entspricht. Der Name der Bedrohung besitzt die Form eines Links zu der Ressource http://www.viruslist.com/de, auf der Sie ausführliche Informationen darüber erhalten können, welche Art von Bedrohung auf Ihrem Computer gefunden wurde.
- Vollständiger Dateiname und Pfad des Prozesses, der die gefährliche Aktivität initiierte.
- Auswahl möglicher Aktionen:
  - **Quarantäne** - Prozess beenden und die ausführbare Datei des Prozesses in die Quarantäne verschieben. Wenn das Objekt in der Quarantäne gespeichert wird, wird es verschoben, nicht kopiert: Die unter Quarantäne stehenden Dateien werden in einem speziellen Format gespeichert und stellen keine Gefahr dar.

    Bei späteren Untersuchungen der Quarantäne mit aktualisierten Bedrohungssignaturen kann sich der Status eines Objekts ändern. Das Objekt kann beispielsweise als infiziert erkannt und mit Hilfe aktualisierter Datenbanken verarbeitet werden, oder es erhält den Status *virenfrei* und kann dann wiederhergestellt werden.

    Wenn sich eine Datei, die manuell in die Quarantäne verschoben wurde, bei einer späteren Untersuchung als virenfrei erweist, ändert sich ihr Status nicht gleich nach der Untersuchung in *ok*. Der Status ändert sich nur dann sofort, wenn die Untersuchung mindestens drei Tage, nachdem die Datei unter Quarantäne gestellt wurde, stattfindet.
  - **Beenden** - Prozess beenden.
  - **Erlauben** - Das Ausführen des Prozesses erlauben.

Damit die ausgewählte Aktion auf alle Objekte mit dem gleichen Status angewendet wird, die während der laufenden Sitzung der Schutzkomponente oder Aufgabe gefunden werden, aktivieren Sie das Kontrollkästchen ☑ **In allen ähnlichen Fällen anwenden**. Als laufende Sitzung gilt die Arbeitszeit einer Komponente ab dem Zeitpunkt ihres Starts

bis zum Moment des Abschaltens oder Neustarts des Programms, sowie die Ausführungszeit einer Untersuchungsaufgabe ab dem Start bis zum Abschluss.

Wenn Sie überzeugt sind, dass das gefundene Programm ungefährlich ist, können Sie es der vertrauenswürdigen Zone hinzufügen, um zu verhindern, dass Kaspersky PURE erneut anspricht, wenn er das Programm findet.

VERSTECKTER PROZESS WURDE GEFUNDEN

Wenn der Proaktive Schutz einen versteckten Prozess im System findet, erscheint auf dem Bildschirm eine spezielle Meldung, die folgende Informationen enthält:

- Name der Bedrohung, der ihrer Bezeichnung in der Viren-Enzyklopädie von Kaspersky Lab entspricht. Der Name der Bedrohung besitzt die Form eines Links zu der Ressource http://www.viruslist.com/de, auf der Sie ausführliche Informationen darüber erhalten können, welche Art von Bedrohung auf Ihrem Computer gefunden wurde.
- Vollständiger Dateiname und Pfad des versteckten Prozesses.
- Auswahl möglicher Aktionen:
  - **Quarantäne** - Die ausführbare Prozessdatei wird in die Quarantäne verschoben. Wenn das Objekt in der Quarantäne gespeichert wird, wird es verschoben, nicht kopiert: Die unter Quarantäne stehenden Dateien werden in einem speziellen Format gespeichert und stellen keine Gefahr dar.

    Bei späteren Untersuchungen der Quarantäne mit aktualisierten Bedrohungssignaturen kann sich der Status eines Objekts ändern. Das Objekt kann beispielsweise als infiziert erkannt und mit Hilfe aktualisierter Datenbanken verarbeitet werden, oder es erhält den Status *virenfrei* und kann dann wiederhergestellt werden.

    Wenn sich eine Datei, die manuell in die Quarantäne verschoben wurde, bei einer späteren Untersuchung als virenfrei erweist, ändert sich ihr Status nicht gleich nach der Untersuchung in *ok*. Der Status ändert sich nur dann sofort, wenn die Untersuchung mindestens drei Tage, nachdem die Datei unter Quarantäne gestellt wurde, stattfindet.
  - **Beenden** - Prozess beenden.
  - **Erlauben** - Das Ausführen des Prozesses erlauben.

Damit die ausgewählte Aktion auf alle Objekte mit dem gleichen Status angewendet wird, die während der laufenden Sitzung der Schutzkomponente oder Aufgabe gefunden werden, aktivieren Sie das Kontrollkästchen ☑ **In allen ähnlichen Fällen anwenden**. Als laufende Sitzung gilt die Arbeitszeit einer Komponente ab dem Zeitpunkt ihres Starts bis zum Moment des Abschaltens oder Neustarts des Programms, sowie die Ausführungszeit einer Untersuchungsaufgabe ab dem Start bis zum Abschluss.

Wenn Sie überzeugt sind, dass das gefundene Programm ungefährlich ist, wird empfohlen, es der vertrauenswürdigen Zone hinzufügen, um zu verhindern, dass Kaspersky PURE erneut anspricht, wenn er das Programm findet.

VERSUCH ZUM ZUGRIFF AUF DIE SYSTEMREGISTRIERUNG WURDE ERKANNT

Wenn der Proaktive Schutz erkennt, dass versucht wird, auf Schlüssel der Systemregistrierung zuzugreifen, erscheint auf dem Bildschirm eine spezielle Meldung, die folgende Informationen enthält:

- Registrierungsschlüssel, auf den der Zugriffsversuch erfolgte.
- Vollständiger Dateiname und Pfad des Prozesses, der versuchte auf Registrierungsschlüssel zuzugreifen.
- Auswahl möglicher Aktionen:

- **Erlauben** - Das Ausführen der gefährlichen Aktion einmal erlauben.
- **Verbieten** - Das Ausführen der gefährlichen Aktion einmal verbieten.

Damit die von Ihnen ausgewählte Aktion jedes Mal automatisch ausgeführt wird, wenn diese Aktivität auf Ihrem Computer initiiert wird, aktivieren Sie das Kontrollkästchen **Regel erstellen**.

Wenn Sie überzeugt sind, dass jede Aktivität der Anwendung, die den Zugriff auf die Systemregistrierungsschlüssel initiierte, ungefährlich ist, fügen Sie diese Anwendung der Liste der vertrauenswürdigen Anwendungen hinzu.

NETZWERKAKTIVITÄT EINES PROGRAMMS WURDE ERKANNT

Wenn die Netzwerkaktivität eines Programms erkannt wird, erscheint auf dem Bildschirm eine Meldung (standardmäßig für Programme der Gruppen **Schwach beschränkt** oder **Stark beschränkt**).

Es wird eine Meldung angezeigt, wenn Kaspersky PURE im interaktiven Modus (s. Abschnitt "Schutzmodus auswählen" auf S. 61), arbeitet und für das Programm, dessen Netzwerkaktivität erkannt wurde, keine Paketregel erstellt wurde.

Die Meldung enthält folgende Informationen:

- Name des Programms und kurze Charakteristik der von ihm initiierten Verbindung.
- Informationen zur Verbindung (Verbindungstyp, lokaler Port und Remoteport, Adresse, mit der die Verbindung erfolgt).
- Startfolge eines Programms.

Ihnen wird angeboten, eine der folgenden Aktionen auszuwählen:

- **Jetzt erlauben**.
- **Jetzt verbieten**.
- **Regel erstellen**. Bei Auswahl dieser Variante öffnet sich das Fenster **Firewall**, in dem Sie eine Regel erstellen können, mit der die Netzwerkaktivität des Programms reguliert wird.

Sie können die Netzwerkaktivität eines Programms einmalig oder für einen längeren Zeitraum verbieten oder erlauben. Führen Sie hierzu eine der folgenden Aktionen aus:

- Um die Netzwerkaktivität eines Programms einmalig zu erlauben oder zu verbieten, wählen Sie bitte **Jetzt erlauben** oder **Jetzt verbieten**.
- Um die ausgewählte Aktion für die gesamte Sitzung des Programms, bei dem eine Netzwerkaktivität festgestellt wurde, zu speichern, wählen Sie **Jetzt erlauben** oder **Jetzt verbieten** aus und aktivieren Sie das Kontrollkästchen **Speichern für diese Programmsitzung**.

  Wird im Fenster das Kontrollkästchen **Speichern für immer** angezeigt, dann aktivieren Sie dieses bitte und betätigen Sie danach den Link **für immer**, um die Bezeichnung in **Speichern für diese Programmsitzung** zu ändern.
- Um die für das Programm ausgewählte Aktion für immer zu speichern, wählen Sie bitte die Aktion **Jetzt erlauben** oder **Jetzt verbieten** und aktivieren Sie das Kontrollkästchen **Speichern für immer**.

  Wird im Fenster das Kontrollkästchen **Speichern für diese Programmsitzung** angezeigt, dann aktivieren Sie dieses bitte und betätigen Sie danach den Link **für die Programmsitzung** zum Ändern der Bezeichnung in **Speichern für immer**.

NEUES NETZWERK WURDE GEFUNDEN

Bei jeder Verbindung des Computers mit einer neuen Zone (Netzwerk) erscheint auf dem Bildschirm eine spezielle Meldung.

Der obere Bereich der Meldung enthält eine kurze Beschreibung des Netzwerks mit Angabe der IP-Adresse und Subnetzmaske.

Im unteren Teil können Sie einen Status für die gefundene Zone festlegen, auf dessen Grundlage entschieden wird, welche Art von Netzwerkaktivität erlaubt wird:

- **Öffentliches Netzwerk (Externen Zugriff auf den Computer verbieten)**. Netzwerk mit hoher Risikostufe. Bei der Arbeit in dieser Zone ist der Computer allen möglichen Typen von Bedrohungen ausgesetzt. Dieser Status wird auch für Netzwerke empfohlen, die nicht durch Antiviren-Programme, Firewalls, Filter usw. geschützt werden. Die Auswahl dieses Status gewährleistet dem Computer bei der Arbeit in dieser Zone maximale Sicherheit.

- **Lokales Netzwerk (Zugriff auf Dateien und Drucker erlauben)**. Es wird empfohlen, diesen Status für Zonen mit mittlerer Risikostufe anzuwenden (beispielsweise für interne Firmennetzwerk).

- **Vertrauenswürdiges Netzwerk (Jede Netzwerkaktivität erlauben)**. Es wird empfohlen, diesen Status nur für absolut sichere Zonen zu verwenden, in denen dem Computer keine Angriffe und Versuche zum unerlaubten Datenzugriff drohen.

PHISHING-ANGRIFF WURDE ERKANNT

Wenn Kaspersky PURE einen Versuch zum Öffnen einer Phishing-Seite entdeckt, erscheint auf dem Bildschirm eine spezielle Meldung.

Die Meldung enthält folgende Informationen:

- Name der Bedrohung – *Phishing-Angriff*. Der Name besitzt die Form eines Links zur Viren-Enzyklopädie von Kaspersky Lab, wo die Bedrohung ausführlich beschrieben wird.

- Web-Adresse der Phishing-Seite im Internet

- Auswahl möglicher Aktionen:

  - **Erlauben** – Download der Phishing-Seite fortsetzen.

  - **Verbieten** – Download der Phishing-Seite blockieren.

Damit die ausgewählte Aktion auf alle Objekte mit dem gleichen Status angewendet wird, die während der laufenden Sitzung der Schutzkomponente oder Aufgabe gefunden werden, aktivieren Sie das Kontrollkästchen **In allen ähnlichen Fällen anwenden**. Als laufende Sitzung gilt die Arbeitszeit einer Komponente ab dem Zeitpunkt ihres Starts bis zum Moment des Abschaltens oder Neustarts des Programms, sowie die Ausführungszeit einer Untersuchungsaufgabe ab dem Start bis zum Abschluss.

VERDÄCHTIGER LINK WURDE GEFUNDEN

Wenn Kaspersky PURE erkennt, dass versucht wird, eine Webseite zu öffnen, deren Adresse auf der Liste der verdächtigen Webadressen steht, erscheint auf dem Bildschirm eine Meldung.

Die Meldung enthält folgende Informationen:

- Webadresse der Seite im Internet.

- Auswahl möglicher Aktionen:

- **Erlauben** – Download der Webseite fortsetzen.
- **Verbieten** – Download der Webseite blockieren.

Damit die ausgewählte Aktion auf alle Objekte mit dem gleichen Status angewendet wird, die während der laufenden Sitzung der Schutzkomponente oder Aufgabe gefunden werden, aktivieren Sie das Kontrollkästchen **In allen ähnlichen Fällen anwenden**. Als laufende Sitzung gilt die Arbeitszeit einer Komponente ab dem Zeitpunkt ihres Starts bis zum Moment des Abschaltens oder Neustarts des Programms, sowie die Ausführungszeit einer Untersuchungsaufgabe ab dem Start bis zum Abschluss.

EIN INKORREKTES ZERTIFIKAT WURDE GEFUNDEN

Die Zuverlässigkeit einer SSL-Verbindung wird mit Hilfe des installierten Zertifikats geprüft. Wenn beim Verbindungsversuch mit einem Server ein inkorrektes Zertifikat verwendet wird (z.B. wenn es von einem Angreifer ausgetauscht wurde), erscheint auf dem Bildschirm eine entsprechende Meldung.

Die Meldung informiert über mögliche Fehlerursachen, Remoteport und Remoteadresse. Sie werden aufgefordert zu entscheiden, ob unter Verwendung des inkorrekten Zertifikats eine Verbindung hergestellt werden soll:

- **Zertifikat akzeptieren** – Verbindung mit der Webressource fortsetzen.
- **Zertifikat ablehnen** – Verbindung mit der Webressource trennen.
- **Zertifikat anzeigen** – Informationen über das Zertifikat anzeigen.

ZEITBESCHRÄNKUNG FÜR DIE VERWENDUNG EINES PROGRAMMS

Wenn in der Kindersicherung eine Zeitbeschränkung für die Verwendung eines Programms besteht, erscheint nach Ablauf der erlaubten Dauer eine entsprechende Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Name des Programms
- Zeit, die bis zum Beenden des Programms verbleibt, oder Grund für das Beenden des Programms

SPEZIELLE DESINFEKTIONSPROZEDUR IST ERFORDERLICH

Beim Fund einer Bedrohung, die gerade im System aktiv ist (beispielsweise ein schädlicher Prozess im Arbeitsspeicher oder in den Autostart-Objekten), erscheint auf dem Bildschirm eine Eingabeaufforderung zum Durchführen einer speziell dafür vorgesehenen erweiterten Desinfektionsprozedur.

Die Spezialisten von Kaspersky Lab empfehlen ausdrücklich, in solchen Fällen die erweiterte Desinfektionsprozedur durchzuführen. Klicken Sie dazu auf **OK**. Beachten Sie aber, dass zum Abschluss des Vorgangs der Computer neu gestartet wird. Deshalb sollten die aktuellen Arbeitsergebnisse gespeichert und alle Anwendungen geschlossen werden, bevor der Vorgang ausgeführt wird.

Während der Desinfektionsvorgang ausgeführt wird, sind der Start von Mailprogrammen und das Ändern der Registrierung des Betriebssystems verboten. Nach dem Neustart des Computers wird empfohlen, die vollständige Virenuntersuchung zu starten.

DIE DATEI IST BEREITS VORHANDEN

Wenn bei der Wiederherstellung aus einer Sicherungskopie im ausgewählten Zielordner bereits eine Datei mit demselben Namen vorhanden ist, erscheint eine entsprechende Meldung auf dem Bildschirm.

Im oberen Bereich der Meldung werden Name und Ort der Datei genannt.

Im unteren Fensterbereich können Sie eine Wiederherstellungsmethode auswählen:

- **Ersetzen**. Vorhandene Datei wird durch wiederherzustellende Datei ersetzt.
- **Überspringen**. Aktuelle Dateiversion wird gespeichert.
- **Beide Dateien speichern**. Wiederherzustellende Datei erhält einen neuen Namen.

GLOSSAR

2

2-Channel-Gateway

Computer mit zwei Netzwerkadaptern, die an verschiedene Netzwerke angeschlossen sind und Daten von einem Netzwerk an ein anderes Netzwerk übermitteln.

A

Aktive Lizenz

Lizenz, die momentan für die Arbeit des Kaspersky-Lab-Programms verwendet wird. Die Lizenz legt die Gültigkeitsdauer für den vollen Funktionsumfang sowie die Lizenzpolitik für das Programm fest. Im Programm kann nur ein Schlüssel den Status "aktiv" besitzen.

Alternative NTFS-Datenströme

Datenströme des NTFS-Dateisystems (alternate data streams), die für zusätzliche Attribute oder Datei-Informationen vorgesehen sind.

Jede Datei im NTFS-Dateisystem stellt eine Auswahl von Datenströmen (streams) dar. In einem Datenstrom befindet sich der Datei-Inhalt, den man sehen kann, wenn man die Datei öffnet, die übrigen (alternativen) Datenströme sind für Meta-Informationen vorgesehen und bieten zum Beispiel die Kompatibilität des NTFS-Systems mit anderen Systemen, wie mit dem alten Dateisystem von Macintosh - Hierarchical File System (HFS). Die Datenströme lassen sich erstellen, löschen, separat speichern, umbenennen und sogar als Prozess starten.

Alternative Datenströme können von Angreifern missbraucht werden, um Daten des Computers heimlich zu übertragen oder zu empfangen.

Anstößige E-Mail

Nachricht, die anstößige Ausdrücke enthält.

Archiv

Datei, die ein oder mehrere Objekte "enthält", die ihrerseits auch Archive sein können.

Aufgabe

Funktionen, die das Kaspersky-Lab-Programm ausführen kann und die als Aufgaben realisiert sind, Beispiele: Echtzeitschutz für Dateien, Vollständige Untersuchung des Computers, Datenbank-Update.

Aufgabeneinstellungen

Parameter für die Arbeit des Programms, die für jeden Aufgabentyp individuell sind.

Ausnahme

Eine Ausnahme ist ein Objekt, das von der Untersuchung durch das Kaspersky-Lab-Programm ausgeschlossen wird. Von der Untersuchung können Dateien eines bestimmten Formats, Dateien nach Maske, bestimmte Bereiche (beispielsweise ein Ordner oder Programm) sowie Programmprozesse oder Objekte nach einem Bedrohungstyp gemäß der Klassifikation der Viren-Enzyklopädie ausgeschlossen werden. Für jede Aufgabe können individuelle Ausnahmen festgelegt werden.

Autostart-Objekte

Auswahl von Programmen, die für den Start und die korrekte Funktion des auf Ihrem Computer installierten Betriebssystems und der vorhandenen Software erforderlich sind. Diese Objekte werden jedes Mal beim Hochfahren des Betriebssystems gestartet. Es gibt Viren, die speziell diese Objekte infizieren können. Dadurch kann beispielsweise das Hochfahren des Betriebssystems blockiert werden.

B

BACKUP

Bevor ein Desinfektionsversuch erfolgt oder die Datei gelöscht wird, legt die Anwendung eine Sicherungskopie an und speichert diese im Backup. Dadurch wird ermöglicht, die Datei bei Bedarf wiederherzustellen, um sie beispielsweise mit aktualisierten Datenbanken zu untersuchen.

BACKUP

Spezieller Speicher für Sicherungskopien von Objekten, die vor einer Desinfektion oder vor dem Löschen angelegt werden.

BENACHRICHTIGUNGSVORLAGE

Vorlage, mit der bei der Untersuchung erkannte infizierte Objekte gemeldet werden. Eine Benachrichtigungsvorlage enthält mehrere Einstellungen, die die Reihenfolge der Benachrichtigung, die Verbreitungsart und den Meldungstext definieren.

BOOTVIRUS

Virus, der die Bootsektoren von Computerlaufwerken infiziert. Der Virus "zwingt" das System beim Hochfahren, nicht auf den eigentlichen Bootcode zuzugreifen, sondern auf den Viruscode, der dann die Kontrolle übernimmt.

C

CONTAINER

Verschlüsseltes Objekt, das für die Speicherung vertraulicher Informationen vorgesehen ist. Ein Container ist ein kennwortgeschützter virtueller Wechseldatenträger, auf dem Dateien und Ordner gespeichert werden.

Um mit Containern arbeiten zu können, muss das Programm Kaspersky PURE auf dem Computer installiert sein.

D

DATEIMASKE

Platzhalter für den Namen und die Erweiterung einer Datei, der aus allgemeinen Zeichen besteht. Die zwei wichtigsten Zeichen, die in Dateimasken verwendet werden sind * und ? (wobei * für eine beliebige Anzahl von beliebigen Zeichen und ? für ein beliebiges Einzelzeichen steht). Mit Hilfe dieser Zeichen kann jede beliebige Datei dargestellt werden. Beachten Sie, dass Name und Endung einer Datei stets durch einen Punkt getrennt werden.

DATENBANK FÜR PHISHING-WEBADRESSEN

Eine Liste der Webressourcen, die von den Kaspersky-Lab-Spezialisten als Phishing-Adressen eingestuft wurden. Die Datenbank wird regelmäßig aktualisiert und gehört zum Lieferumfang des Kaspersky-Lab-Programms.

DATENBANK FÜR VERDÄCHTIGE WEBADRESSEN

Eine Liste der Webressourcen, deren Inhalt als potentiell gefährlich eingestuft werden kann. Die Liste ist von den Kaspersky-Lab-Spezialisten angelegt, wird regelmäßig aktualisiert und gehört zum Lieferumfang des Programms.

DATENBANK-UPDATE

Eine Funktion, die vom Kaspersky-Lab-Programm ausgeführt wird und die es erlaubt, den aktuellen Zustand des Schutzes aufrecht zu erhalten. Dabei werden die Datenbanken von den Kaspersky-Lab-Updateservern auf den Computer kopiert und automatisch von der Anwendung übernommen.

DATENBANKEN

Datenbanken, die von den Kaspersky-Lab-Spezialisten gepflegt werden und eine genaue Beschreibung aller momentan existierenden Bedrohungen der Computersicherheit sowie Methoden zu ihrer Identifikation und Desinfektion enthalten. Die Datenbanken werden von Kaspersky Lab laufend aktualisiert, wenn neue Bedrohungen auftauchen.

DESINFEKTION VON OBJEKTEN

Methode zur Bearbeitung von infizierten Objekten, bei der die Daten vollständig oder teilweise wiederhergestellt werden oder eine Entscheidung darüber getroffen wird, dass die Desinfektion von Objekten nicht möglich ist. Die Desinfektion von Objekten erfolgt auf Basis der Einträge in den Datenbänken. Bei der Desinfektion können Daten teilweise verloren gehen.

DESINFEKTION VON OBJEKTEN BEIM NEUSTART

Methode zur Verarbeitung von infizierten Objekten, die im Augenblick der Desinfektion von anderen Programmen verwendet werden. Dabei wird eine Kopie des infizierten Objekts angelegt. Beim folgenden Neustart wird die Kopie desinfiziert und das infizierte Originalobjekt wird durch die desinfizierte Kopie ersetzt.

DOMAIN NAME SERVICE (DNS)

Verbreitetes System zur Umformung von Hostnamen (Computer oder anderes Netzwerkgerät) in eine IP-Adresse. DNS funktioniert in TCP/IP-Netzwerken. Im Einzelfall kann DNS auch umgekehrte Anfragen und Definitionen von Hostnamen nach dessen IP (PTR-Eintrag) speichern und verarbeiten. Die Auflösung von DNS-Namen erfolgt gewöhnlich durch Netzwerkprogramme und nicht durch die Benutzer.

DRINGENDES UPDATE

Kritisches Update für die Module des Kaspersky-Lab-Programms.

E

E-MAIL LÖSCHEN

Verarbeitungsmethode für eine E-Mail, bei der die Nachricht physikalisch gelöscht wird. Diese Methode wird für E-Mails empfohlen, die eindeutig Spam oder ein schädliches Objekt enthalten. Vor dem Löschen einer Nachricht, wird ihre Kopie im Backup gespeichert (wenn diese Funktion nicht deaktiviert wurde).

ECHTZEITSCHUTZ

Funktionsmodus des Programms, in dem Objekte im Echtzeitmodus auf schädlichen Code untersucht werden.

Das Programm fängt jeden Versuch zum Öffnen, Schreiben und Ausführen eines Objekts ab, und durchsucht das Objekt nach Bedrohungen. Virenfreie Objekte werden für den Zugriff freigegeben, infizierte oder verdächtige Objekte werden gemäß den Aufgabenparametern verarbeitet (desinfiziert, gelöscht, in die Quarantäne verschoben).

EIN- UND AUSGABEPORT

Wird in Mikroprozessoren (z.B. Intel) beim Datenaustausch mit der Hardware verwendet. Der Ein- und Ausgabeport wird einem bestimmten Gerät zugeordnet und erlaubt es den Programmen, zum Datenaustausch darauf zuzugreifen.

EMPFOHLENE STUFE

Sicherheitsstufe, deren Funktionsparameter von Kaspersky Lab empfohlen werden und die einen optimalen Schutz Ihres Computers gewährleistet. Diese Stufe wird in der Grundeinstellung verwendet.

F

FEHLALARM

Situation, in der ein virenfreies Objekt von der Kaspersky-Lab-Anwendung als infiziert eingestuft wird, weil sein Code Ähnlichkeit mit einem Virus aufweist.

G

GEFÄHRLICHES OBJEKT

Objekt, in dem sich ein Virus befindet. Es wird davor gewarnt, mit solchen Objekten zu arbeiten, weil dies zur Infektion des Computers führen kann. Beim Fund eines infizierten Objekts wird empfohlen, das Objekt mit Hilfe des Kaspersky-Lab-Programms zu desinfizieren oder, falls die Desinfektion nicht möglich ist, es zu löschen.

GEPACKTE DATEI

Archivdatei, die ein Extrahierprogramm und für das Betriebssystem bestimmte Extrahierbefehle enthält.

GÜLTIGKEITSDAUER DER LIZENZ

Zeitraum, für den Sie berechtigt sind, das Kaspersky-Lab-Programm mit allen Funktionen zu nutzen. Die Gültigkeitsdauer der Lizenz beträgt in der Regel ein Kalenderjahr ab der Installation der Lizenz. Wenn die Gültigkeitsdauer der Lizenz abgelaufen ist, wird die Funktionalität des Programms eingeschränkt: Das Update der Datenbanken ist nicht mehr verfügbar.

H

HARDWARE-PORT

Eingang an einem Hardware-Element des Computers, an den ein Kabel oder ein Stecker angeschlossen werden kann (LPT-Port, serieller Port, USB).

HEURISTISCHE ANALYSE

Technologie zum Erkennen von Bedrohungen, die nicht mit Hilfe der Datenbanken für Kaspersky-Lab-Programme identifiziert werden können. Es wird erlaubt, Objekte zu finden, die verdächtig sind, durch einen unbekannten Virus oder eine neue Modifikation eines bekannten Virus infizierte zu sein.

Mit Hilfe der heuristischen Analyse werden bis zu 92 % der neuen Bedrohungen erkannt. Dieser Mechanismus ist sehr effektiv und führt nur selten zu einem Fehlalarm.

Dateien, die mit Hilfe der heuristischen Analyse gefunden werden, nennt man verdächtig.

I

ICHECKER-TECHNOLOGIE

Diese Technologie erlaubt eine Erhöhung der Untersuchungsgeschwindigkeit. Dabei werden jene Objekte von der Untersuchung ausgeschlossen, die seit dem vorherigen Scannen nicht verändert wurden, wobei vorausgesetzt wird, dass die Untersuchungsparameter (Antiviren-Datenbanken und Einstellungen) gleich geblieben sind. Informationen darüber werden einer speziellen Datenbank aufgezeichnet. Die Technologie wird sowohl für den Echtzeitschutz als auch für den Scan auf Befehl verwendet.

Wurde beispielsweise eine Archivdatei vom Programm untersucht und ihr wurde der Status virenfrei zugewiesen. Dann wird das Archiv von der folgenden Untersuchung ausgeschlossen, wenn es nicht verändert wurde und die Untersuchungsparameter gleich geblieben sind. Wenn seit der letzten Untersuchung die Zusammensetzung des Archivs durch Hinzufügen eines neuen Objekts verändert wurde, die Untersuchungsparameter geändert oder die Programm-Datenbanken aktualisiert wurden, wird das Archiv erneut untersucht.

Einschränkungen der Technologie iChecker:

- Die Technologie funktioniert nicht mit großen Dateien, da die Untersuchung der gesamten Datei in diesem Fall weniger Zeit beansprucht, als zu ermitteln, ob sie seit der letzten Untersuchung verändert wurde.
- Die Technologie unterstützt eine begrenzte Anzahl von Formaten (**exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar**).

INDIKATOR FÜR EINE VIRENEPIDEMIE

Vorlage, auf der eine Benachrichtigung über den drohenden Ausbruch einer Virenepidemie beruht. Der Indikator für eine Virenepidemie umfasst einige Einstellungen, die den Schwellenwert der Virenaktivität, die Verbreitungsart und den Meldungstext enthalten.

INFIZIERTES OBJEKT

Objekt, das schädlichen Code enthält: Bei der Untersuchung des Objekts wurde erkannt, dass ein Abschnitt des Objektcodes vollständig mit dem Code einer bekannten Bedrohung übereinstimmt. Die Kaspersky-Lab-Spezialisten warnen davor, mit solchen Objekten zu arbeiten, weil dies zur Infektion Ihres Computers führen kann.

INKOMPATIBLES PROGRAMM

Antiviren-Programm eines Drittherstellers oder Kaspersky-Lab-Programm, das nicht mit Kaspersky PURE verwaltet werden kann.

INSTALLATION MIT LOGIN-SZENARIO

Remote-Installation von Kaspersky-Lab-Programmen, mit der der Start der Aufgabe zur Remote-Installation mit einem konkreten Benutzerkonto (mehreren Benutzerkonten) verknüpft werden kann. Beim Anmelden des Benutzers in der Domäne wird versucht, das Programm auf dem Client-Computer zu installieren, auf dem sich der Benutzer angemeldet hat. Dieses Verfahren wird für die Installation von Programmen des Herstellers auf Computern empfohlen, die mit den Betriebssystemen Microsoft Windows 98 / Me laufen.

INTERCEPTOR

Subkomponente des Programms, die für die Untersuchung bestimmter Typen von E-Mails verantwortlich ist. Die Auswahl der zu installierenden Interceptoren ist davon abhängig, in welcher Rolle oder Rollenkombination das Programm eingesetzt werden soll.

INTERNETPROTOKOLL (IP)

Basisprotokoll für das Internet, das seit seiner Entwicklung im Jahre 1974 unverändert verwendet wird. Es führt die Grundoperationen bei der Datenübertragung von einem Computer auf einen anderen aus und dient als Basis für alle Protokolle höherer Ebenen wie TCP und UDP. Es kontrolliert die Verbindung und die Fehlerbehandlung. Technologien wie IPv4 und Maskierung ermöglichen es, umfangreiche Netzwerke hinter einer relativ geringen Anzahl von IP-Adressen zu verbergen (oder sogar hinter einer Adresse). Dadurch wird erlaubt, die Ansprüche des ständig expandierenden Internets unter Verwendung eines relativ begrenzten IPv4-Adressraums zu befriedigen.

K

KASPERSKY-LAB-UPDATESERVER

Liste der http- und ftp-Server von Kaspersky Lab, von denen das Programm die Updates für Datenbanken und Module auf Ihren Computer herunterlädt.

KONTROLLIERTES OBJEKT

Datei, die mit den Protokollen HTTP, FTP oder SMTP übertragen und von der Firewall zur Untersuchung durch das Kaspersky-Lab-Programm umgeleitet wird.

KOPFZEILE (HEADER)

Informationen, die am Anfang einer Datei oder E-Mail stehen und Basisdaten über Status und Verarbeitung der Datei (E-Mail) enthalten. Die Kopfzeile einer E-Mail enthält z.B. Angaben über Absender, Empfänger und Datum.

L

LAUFWERKSBOOTSEKTOR

Ein Bootsektor ist ein spezieller Sektor auf der Festplatte eines Computers, auf einer Diskette oder auf einem anderen Gerät zur Datenspeicherung. Er enthält Angaben über das Dateisystem des Datenträgers und ein Bootprogramm, das für den Start des Betriebssystems verantwortlich ist.

Laufwerksbootsektoren können von so genannten Bootviren infiziert werden. Die Kaspersky-Lab-Anwendung erlaubt es, Bootsektoren auf Viren zu untersuchen und infizierte Sektoren zu desinfizieren.

LISTE DER VERTRAUENSWÜRDIGEN WEBADRESSEN

Eine Liste der Masken und Webressourcen, deren Inhalt der Benutzer vertraut. Webseiten, die einem Element dieser Liste entsprechen, werden vom Kaspersky-Lab-Programm auf das Vorhandensein schädlicher Objekte nicht untersucht.

LISTE DER ZU UNTERSUCHENDEN WEBADRESSEN

Eine Liste der Masken und Webressourcen, die vom Kaspersky-Lab-Programm auf das Vorhandensein schädlicher Objekte unbedingt untersucht werden sollen.

LISTE MIT ERLAUBTEN ABSENDERN

(auch Weiße Adressenliste)

Liste mit E-Mail-Adressen. Die von diesen Adressen eintreffenden Nachrichten werden nicht vom Kaspersky-Lab-Programm untersucht.

LISTE MIT ERLAUBTEN WEBADRESSEN

Eine Liste der Masken und Webressourcen, auf die der Zugriff vom Kaspersky-Lab-Programm nicht blockiert wird. Eine Adressenliste wird vom Benutzer bei der Programmkonfiguration erstellt.

LISTE MIT VERBOTENEN ABSENDERN

(auch Schwarze Adressenliste)

Liste mit E-Mail-Adressen. Die von diesen Adressen eintreffenden Nachrichten werden vom Kaspersky-Lab-Programm ungeachtet ihres Inhalts blockiert .

LISTE MIT VERBOTENEN WEBADRESSEN

Eine Liste der Masken und Webressourcen, auf die der Zugriff vom Kaspersky-Lab-Programm blockiert wird. Eine Adressenliste wird vom Benutzer bei der Programmkonfiguration erstellt.

M

MAIL-DATENBANKEN

Datenbanken mit einem speziellem Format, in denen die auf Ihrem Computer gespeicherten E-Mails enthalten sind. Jede eingehende/ausgehende E-Mail wird nach dem Empfang/Senden in einer Mail-Datenbank gespeichert. Solche Datenbanken werden bei einer vollständigen Untersuchung des Computers untersucht.

Eingehende und ausgehende E-Mails werden im Augenblick des Empfangs und Sendens in Echtzeit auf Viren analysiert, wenn der Echtzeitschutz aktiviert ist.

MÖGLICHERWEISE INFIZIERTES OBJEKT

Objekt, dessen Code entweder den modifizierten Code eines bekannten Virus oder einen Code, der einem Virus gleicht, enthält, der Kaspersky Lab aber bisher nicht bekannt ist. Infizierte Dateien können mit Hilfe der heuristischen Analyse gefunden werden.

N

NETZWERKPORT

Parameter für die Protokolle TCP und UDP, der den Zweck von Datenpaketen im IP-Format definiert, die über ein Netzwerk auf einen Host übertragen werden. Er erlaubt unterschiedlichen auf einem Host ausgeführten Programmen, unabhängig voneinander Daten zu empfangen. Jedes Programm verarbeitet die Daten, die auf einem bestimmten Port eintreffen (man sagt auch, ein Programm "hört" einen bestimmten Port).

Gewöhnlich sind häufig verwendeten Netzwerkprotokollen standardmäßige Portnummern zugeordnet (Webserver empfangen ihre Daten standardmäßig mit dem HTTP-Protokoll auf TCP-Port 80), obwohl ein Programm prinzipiell ein beliebiges Protokoll und einen beliebigen Port verwenden kann. Mögliche Werte: von 1 bis 65535.

O

OLE-OBJEKT

Objekt, das an eine andere Datei angehängt oder darin eingebettet ist. Das Kaspersky-Lab-Programm erlaubt es, OLE-Objekte auf das Vorhandensein von Viren zu untersuchen. Wenn Sie beispielsweise eine beliebige Tabelle aus Microsoft Office Excel in ein Dokument des Typs Microsoft Office Word einfügen, wird die Tabelle als OLE-Objekt untersucht.

OBJEKT BLOCKIEREN

Der Zugriff externer Programme auf ein Objekt wird verboten. Ein blockiertes Objekt kann nicht gelesen, ausgeführt, verändert oder gelöscht werden.

OBJEKT LÖSCHEN

Methode zur Objektbearbeitung, bei der das Objekt physikalisch von dem Ort gelöscht wird, an dem es vom Programm gefunden wurde (Festplatte, Ordner, Netzwerkressource). Diese Bearbeitungsmethode wird für gefährliche Objekte empfohlen, deren Desinfektion aus bestimmten Gründen nicht möglich ist.

OBJEKTE IN DIE QUARANTÄNE VERSCHIEBEN

Verarbeitungsmethode für ein möglicherweise infiziertes Objekt. Dabei wird der Zugriff auf das Objekt gesperrt und das Objekt wird vom ursprünglichen Speicherort in den Quarantäneordner verschoben. Dort wird es in verschlüsselter Form gespeichert, um eine Infektion auszuschließen.

P

POTENTIELL INFIZIERBARES OBJEKT

Ein Objekt das aufgrund seiner Struktur seines Formats von einem Angreifer als "Container" benutzt werden kann, um ein schädliches Objekt zu platzieren oder weiterzuverbreiten. In der Regel sind dies ausführbare Dateien mit Erweiterungen wie com, exe, dll usw. Das Risiko des Eindringens und der Aktivierung von schädlichem Code ist für solche Dateien relativ hoch.

PRIORITÄTSSTUFE FÜR EIN EREIGNIS

Merkmal eines Ereignisses, das bei der Arbeit der Kaspersky-Lab-Anwendung eingetreten ist. Es gibt vier Prioritätsstufen:

- **Kritisches Ereignis**
- **Funktionsstörung**
- **Warnung**
- **Informative Meldung**

Ereignisse des gleichen Typs können unterschiedliche Prioritätsstufen besitzen. Entscheidend ist die Situation, in der ein Ereignis eintritt.

PROGRAMM AKTIVIEREN

Freischalten aller Programmfunktionen. Für die Aktivierung des Programms benötigt der Benutzer eine Lizenz.

PROGRAMM-MODULE

Dateien, die zum Lieferumfang von Kaspersky Lab gehören und für die Realisierung der wichtigsten Aufgaben zuständig sind. Jeder Art von Aufgaben, die das Programm realisiert (Echtzeitschutz, Virensuche, Update), entspricht ein eigenes ausführbares Modul. Wenn die vollständige Untersuchung Ihres Computers aus dem Hauptfenster gestartet wird, initiieren Sie den Start des Moduls für diese Aufgabe.

PROGRAMMEINSTELLUNGEN

Einstellungen für die Arbeit des Programms, die für alle Aufgabentypen gleich sind und sich auf das gesamte Programm beziehen, zum Beispiel Parameter für die Leistungsfähigkeit des Programms, Parameter für das Berichtswesen, Backup-Parameter.

PROTOKOLL.

Genau definierte und standardisierte Kombination von Regeln, die das Verhältnis zwischen Client und Server regulieren. Bekannte Protokolle und die entsprechenden Dienste sind z.B. HTTP (WWW), FTP und NNTP (News).

PROXYSERVER

Dienst in Computernetzwerken, mit dem Clients indirekte Anfragen an anderen Netzwerkserives richten können. Zunächst baut der Client eine Verbindung zu einem Proxyserver auf und fragt nach einer bestimmten Ressource (zum Beispiel nach einer Datei), die auf einem anderen Server liegt. Dann stellt der Proxyserver mit dem angegebenen Server eine Verbindung her und nimmt von ihm die Ressource entgegen oder schreibt die Ressource in seinen eigenen Cache (falls der Proxy einen Cache besitzt). In einigen Fällen kann die Client-Anfrage oder Server-Antwort vom Proxyserver zu bestimmten Zwecken geändert werden.

Q

QUARANTÄNE

Ein bestimmter Ordner, in den alle möglicherweise infizierten Objekte verschoben werden, die bei der Untersuchung oder im Rahmen des Echtzeitschutzes gefunden werden.

R

RESERVELIZENZ

Lizenz, die für die Arbeit der Kaspersky-Lab-Anwendung hinzugefügt, aber nicht aktiviert wurde. Eine Reservelizenz wird aktiviert, wenn die Gültigkeit der aktiven Lizenz abläuft.

S

SOCKS

Proxyserver-Protokoll, mit dem eine zweiseitige Verbindung zwischen Computern eines lokalen und externen Netzwerks realisiert werden kann.

SCHLÜSSELDATEI

Datei mit der Endung .key, die Ihr persönlicher "Schlüssel" ist und für die Arbeit des Kaspersky-Lab-Programms erforderlich ist. Eine Schlüsseldatei ist im Lieferumfang des Produkts enthalten, wenn es bei einem Händler von Kaspersky Lab erworben wurde, oder sie wird Ihnen per E-Mail zugesandt, wenn das Produkt in einem Internet-Shop gekauft wurde.

SCHUTZSTATUS

Aktueller Schutzstatus, der das Sicherheitsniveau des Computers charakterisiert.

SCHWARZE LISTE FÜR SCHLÜSSELDATEIEN

Datenbank mit Informationen über die von Kaspersky Lab blockierten Schlüsseldateien. Die Datei mit der Schwarzen Liste wird gemeinsam mit den Datenbanken aktualisiert.

SCHWELLE FÜR VIRENAKTIVITÄT

Maximal zulässige Anzahl von Ereignissen eines bestimmten Typs innerhalb eines festgelegten Zeitraums, deren Überschreitung als erhöhte Virenaktivität und als Anzeichen eines Virenangriffs gilt. Dieser Wert besitzt insbesondere bei Viren-Epidemien große Bedeutung und erlaubt es dem Administrator, rechtzeitig auf drohende Virenangriffe zu reagieren.

SICHERHEITSSTUFE

Unter Sicherheitsstufe wird eine vordefinierte Auswahl von Parametern für die Arbeit einer Komponente verstanden.

SKRIPT

Ein kleines Computerprogramm oder ein unabhängiger Programmteil (Funktion), das/der in der Regel dazu dient, eine konkrete Aufgabe auszuführen. Meistens werden sie bei Programmen, die in Hypertext integriert sind, verwendet. Skripts werden beispielsweise gestartet, wenn Sie eine bestimmte Webseite öffnen.

Wenn der Echtzeitschutz aktiviert ist, überwacht die Anwendung den Start von Skripts, fängt sie ab und untersucht diese auf Viren. Abhängig von den Untersuchungsergebnissen können Sie die Ausführung eines Skripts verbieten oder erlauben.

SPAM

Unerwünschte massenhafte Versendung von E-Mails, die meistens Werbung enthalten.

SUBNETZMASKE

Die Subnetzmaske (auch Netzwerkmaske genannt) und die Netzwerkadresse definieren die Adressen der Computer, die zu einem Netzwerk gehören.

U

UNBEKANNTER VIRUS

Neuer Virus, über den noch keine Informationen in den Datenbanken vorhanden sind. Unbekannte Viren werden mit der heuristischen Analyse erkannt und erhalten den Status möglicherweise infiziert.

UNTERSUCHUNG DES DATENVERKEHRS

Untersuchung von Objekten, die mit beliebigen Protokollen übertragen werden (z.B. HTTP, FTP u.a.). Die Untersuchung erfolgt im Echtzeitmodus unter Verwendung der aktuellen (letzten) Datenbankversion.

UPDATE

Vorgang, bei dem vorhandene Dateien (Datenbanken oder Programm-Module) durch neue Dateien ersetzt bzw. neue Dateien hinzugefügt werden. Die neuen Dateien werden von den Kaspersky-Lab-Updateservern heruntergeladen.

UPDATEPAKET

Dateipaket, das der Softwareaktualisierung dient, aus dem Internet kopiert und auf Ihrem Computer installiert wird.

V

VERDÄCHTIGE E-MAIL

E-Mail, die sich nicht eindeutig als Spam einstufen lässt, bei deren Untersuchung sich aber ein Verdacht ergeben hat (z.B. bestimmte Arten von Massenmails und Werbenachrichten).

VERDÄCHTIGES OBJEKT

Objekt, dessen Code entweder den modifizierten Code eines bekannten Virus oder einen Code, der einem Virus gleicht, enthält, der Kaspersky Lab aber bisher nicht bekannt ist. Verdächtige Objekte werden unter Einsatz der heuristischen Analyse erkannt.

VERFÜGBARES UPDATE

Updatepaket für die Module einer Kaspersky-Lab-Anwendung, das dringende Updates, die über einen bestimmten Zeitraum gesammelt wurden, sowie Änderungen der Anwendungsarchitektur enthält.

VERTRAUENSWÜRDIGER PROZESS

Programmprozess, dessen Dateioperationen im Echtzeitschutz nicht von der Kaspersky-Lab-Anwendung kontrolliert werden. Das bedeutet, dass alle von einem vertrauenswürdigen Prozess gestarteten, geöffneten und gespeicherten Objekte nicht untersucht werden.

VIRENANGRIFF

Eine Reihe zielgerichteter Versuche, einen Computer mit einem Virus zu infizieren.

W

WIEDERHERSTELLUNG

Ein Originalobjekt wird aus der Quarantäne oder aus dem Backup entweder an den ursprünglichen Ort, an dem das Objekt gespeichert war, bevor es in die Quarantäne verschoben, desinfiziert oder gelöscht wurde, oder in einen benutzerdefinierten Ordner verschoben.

Z

ZERTIFIKAT DES ADMINISTRATIONSSERVERS

Zertifikat, mit dem der Administrationsserver beim Herstellen einer Verbindung mit der Administrationskonsole und Datenaustausch mit den Client-Computern authentifiziert wird. Das Zertifikat des Administrationsservers wird bei Installation des Administrationsservers angelegt und im Unterordner Cert des Installtionsverzeichnisses gespeichert.

KASPERSKY LAB

Kaspersky Lab wurde 1997 gegründet. Heute sind wir das bekannteste Unternehmen für Datenschutz-Software in Russland und bieten eine breite Palette an: Programmen zum Schutz vor Viren, unerwünschten E-Mails (Spam) und Hackerangriffen.

Kaspersky Lab ist ein international operierender Konzern. Die Zentrale befindet sich in Russland, es gibt Niederlassungen in Großbritannien, Frankreich, Deutschland, Japan, in den Benelux-Ländern, China, Polen, Rumänien und in den USA (Kalifornien). In Frankreich wurde eine neue Tochtergesellschaft gegründet, das Europäische Zentrum für Antiviren-Forschung. Unser Partnernetzwerk vereint weltweit mehr als 500 Unternehmen.

Kaspersky Lab – das sind heute mehr als tausend hoch qualifizierte Fachleute, von denen ein Dutzend MBA-Diplome und sechzehn einen Doktortitel besitzen. Die führenden Virusanalytiker von Kaspersky Lab gehören zur prestigeträchtigen Computer Anti-virus Researcher's Organization (CARO).

Das größte Kapital des Unternehmens sind das einzigartige Wissen und die Erfahren, die die Mitarbeiter im Laufe des mehr als vierzehnjährigen ununterbrochenen Kampfes gegen Viren gesammelt haben. Dank der ständigen Analyse von Virenaktivitäten können wir Tendenzen bei der Malware-Entwicklung vorhersagen und frühzeitig Benutzern einen zuverlässigen Schutz vor neuen Angriffen an die Hand geben. Dieser einzigartige Vorteil bildet die Basis der Produkte und Dienstleistungen von Kaspersky Lab. Wir sind unseren Wettbewerbern stets einen Schritt voraus und bieten unseren Kunden den besten Schutz.

Aufgrund der jahrelangen Tätigkeit wurde das Unternehmen zum führenden Entwickler von Technologien zum Schutz vor Viren. Kaspersky Lab hat als erstes Unternehmen viele moderne Standards für Antiviren-Software gesetzt. Die Basis-Software des Unternehmens heißt Kaspersky Anti-Virus und sie sorgt für einen zuverlässigen Schutz aller Objekte vor Virenangriffen: Arbeitsstationen, Dateiserver, Mail-Systeme, Firewalls und Internet-Gateways sowie Taschencomputer. Bequeme Steuerelemente versetzen die Benutzer in die Lage, den Antivirenschutz von Computern und Unternehmensnetzwerken maximal zu automatisieren. Viele internationale Developer verwendeten in ihrer Software den Kernel von Kaspersky Anti-Virus, beispielsweise: Nokia ICG (USA), Aladdin (Israel), Sybari (USA), G Data (Deutschland), Deerfield (USA), Alt-N (USA), Microworld (Indien), BorderWare (Kanada).

Die Kunden von Kaspersky Lab kommen in den Genuss eines breiten Spektrums von Zusatzleistungen, die das störungsfreie Funktionieren der Erzeugnisse und die genaue Kompatibilität mit speziellen Business-Vorgaben garantieren. Wir projektieren, realisieren und begleiten Antiviren-Komplex-Lösungen von Unternehmen. Unsere Datenbanken werden stündlich aktualisiert. Wir haben für unsere Benutzer einen technischen Kundendienst in mehreren Sprachen eingerichtet.

Sollten Sie weitere Informationen wünschen, wenden Sie sich bitte an unsere Vertriebspartner oder direkt an Kaspersky Lab. Wir beraten Sie gern detailliert über das Telefon oder E-Mail. Auf Ihre Fragen bekommen Sie eine vollständige und erschöpfende Antwort.

Webseite von Kaspersky Lab:	http://www.kaspersky.de
Viren-Enzyklopädie:	http://www.securelist.com/de/
Antiviren-Labor:	newvirus@kaspersky.com (nur zum Einsenden verdächtiger Objekte, die zuvor archiviert wurden) http://support.kaspersky.ru/virlab/helpdesk.html?LANG=de (für Fragen an die Virenanalytiker)
Webforum von Kaspersky Lab:	http://forum.kaspersky.com

INFORMATIONEN ZUM CODE VON DRITTHERSTELLERN

Bei der Entwicklung des Programms wurde der Code von Drittherstellern verwendet.

IN DIESEM ABSCHNITT

Programmcode 287

Sonstige Informationen 310

PROGRAMMCODE

Informationen zum Programmcode von Drittherstellern, der bei der Entwicklung des Programms verwendet wurde.

IN DIESEM ABSCHNITT

AGG (ANTI-GRAIN GEOMETRY) 2.4 288
BISON PARSER SKELETON 2.3 289
BOOST 1.30.0, 1.39.0, 1.43.0 289
BZIP2/LIBBZIP2 1.0.5 290
EXPAT 1.2, 2.0.1 290
FASTSCRIPT 1.9 290
GECKO SDK 1.8 290
INFO-ZIP 5.51 290
LIBJPEG 6B 291
LIBNKFM 2.0.5 292
LIBPNG 1.2.8, 1.2.29 292
LIBSPF2 1.2.9 292
LIBUNGIF 3.0 293
LIBXDR 293
NDIS INTERMEDIATE MINIPORTDRIVER SAMPLE 293
NDIS SAMPLE NDIS LIGHTWEIGHT FILTER DRIVER 294
NETWORK CONFIGURATION SAMPLE 294
OPENSSL 0.9.8D 294
PCRE 3.0, 7.4, 7.7 295
PROTOCOL BUFFER 296
QT 4.6.1 296
RFC1321-BASED (RSA-FREE) MD5 LIBRARY 302
TINICONV 1.0.0 302
WINDOWS TEMPLATE LIBRARY 7.5 307
WINDOWS TEMPLATE LIBRARY 8.0 310
ZLIB 1.2, 1.2.2 310

AGG (ANTI-GRAIN GEOMETRY) 2.4

Copyright (C) 2002-2005, Maxim Shemanarev

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 2004 Alberto Demichelis

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

BISON PARSER SKELETON 2.3

Copyright (C) GNU Project

---

http://ftp.gnu.org/gnu/bison/

As a special exception, you may create a larger work that containspart or all of the Bison parser skeleton and distribute that work under terms of your choice, so long as that work isn't itself a parser generator using the skeleton or a modified version thereof as a parser skeleton. Alternatively, if you modify or redistribute the parser skeleton itself, you may (at your option) remove this special exception, which will cause the skeleton and the resulting Bison output files to be licensed under the GNU General Public License without this special exception.

BOOST 1.30.0, 1.39.0, 1.43.0

Copyright (C) Beman Dawes

BZIP2/LIBBZIP2 1.0.5

Copyright (C) 1996-2007, Julian R Seward

EXPAT 1.2, 2.0.1

Copyright (C) 1998, 1999, 2000, Thai Open Source Software Center Ltd

----

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

FASTSCRIPT 1.9

Copyright (C) Fast Reports Inc

GECKO SDK 1.8

Copyright (C) Mozilla Foundation

----

http://www.mozilla.org/MPL/MPL-1.1.html

INFO-ZIP 5.51

Copyright (C) 1990-2007, Info-ZIP

This software is provided "as is", without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the above disclaimer and the following restrictions:

1. Redistributions of source code (in whole or in part) must retain the above copyright notice, definition, disclaimer, and this list of conditions.

2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP--must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.

4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip, "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

LIBJPEG 6B

Copyright (C) 1991-2009, Thomas G. Lane, Guido Vollbeding

LEGAL ISSUES

In plain English:

We don't promise that this software works. (But if you find any bugs, please let us know!)

You can use this software for whatever you want. You don't have to pay us.

You may not pretend that you wrote this software. If you use it in a program, you must acknowledge somewhere in your documentation that you've used the IJG code.

In legalese:

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

(1) If any part of the source code for this software is distributed, then this README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.

(2) If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".

(3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

ansi2knr.c is included in this distribution by permission of L. Peter Deutsch, sole proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA. ansi2knr.c is NOT covered by the above copyright and conditions, but instead by the usual distribution terms of the Free Software Foundation; principally, that you must include source code if you redistribute it. (See the file ansi2knr.c for full details.) However, since ansi2knr.c is not needed as part of any program generated from the IJG code, this does not limit you more than the foregoing paragraphs do.

The Unix configuration script "configure" was produced with GNU Autoconf. It is copyright by the Free Software Foundation but is freely distributable. The same holds for its supporting scripts (config.guess, config.sub, ltconfig, ltmain.sh). Another support script, install-sh, is copyright by M.I.T. but is also freely distributable.

It appears that the arithmetic coding option of the JPEG spec is covered by patents owned by IBM, AT&T, and Mitsubishi. Hence arithmetic coding cannot legally be used without obtaining one or more licenses. For this reason, support for arithmetic coding has been removed from the free JPEG software.

(Since arithmetic coding provides only a marginal gain over the unpatented Huffman mode, it is unlikely that very many implementations will support it.) So far as we are aware, there are no patent restrictions on the remaining code.

The IJG distribution formerly included code to read and write GIF files. To avoid entanglement with the Unisys LZW patent, GIF reading support has been removed altogether, and the GIF writer has been simplified to produce "uncompressed GIFs". This technique does not use the LZW algorithm; the resulting GIF files are larger than usual, but are readable by all standard GIF decoders.

We are required to state that "The Graphics Interchange Format(c) is the Copyright property of CompuServe Incorporated. GIF(sm) is a Service Mark property of CompuServe Incorporated."

LIBNKFM 2.0.5

Copyright (C) KUBO Takehiro

LIBPNG 1.2.8, 1.2.29

Copyright (C) 2004, 2006-2008, Glenn Randers-Pehrson

LIBSPF2 1.2.9

Copyright (C) 2005, Shevek and Wayne Schlitt

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,

STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

LIBUNGIF 3.0

Copyright (C) 1997, Eric S. Raymond

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LIBXDR

Copyright (C) Sun Microsystems, Inc

Sun RPC is a product of Sun Microsystems, Inc. and is provided for unrestricted use provided that this legend is included on all tape media and as a part of the software program in whole or part.

Users may copy or modify Sun RPC without charge, but are not authorized to license or distribute it to anyone else except as part of a product or program developed by the user.

SUN RPC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE WARRANTIES OF DESIGN, MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

Sun RPC is provided with no support and without any obligation on the part of Sun Microsystems, Inc. to assist in its use, correction, modification or enhancement.

SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY SUN RPC OR ANY PART THEREOF.

In no event will Sun Microsystems, Inc. be liable for any lost revenue or profits or other special, indirect and consequential damages, even if Sun has been advised of the possibility of such damages.

Sun Microsystems, Inc.

2550 Garcia Avenue

Mountain View, California 94043

NDIS INTERMEDIATE MINIPORTDRIVER SAMPLE

Copyright (C) 1992-2000, Microsoft Corporation

NDIS SAMPLE NDIS LIGHTWEIGHT FILTER DRIVER

Copyright (C) 2004-2005, Microsoft Corporation

NETWORK CONFIGURATION SAMPLE

Copyright (C) 1997, Microsoft Corporation

OPENSSL 0.9.8D

Copyright (C) 1998-2007, The OpenSSL Project

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)")"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com). Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:"This product includes cryptographic software written byEric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence

[including the GNU Public Licence.]

PCRE 3.0, 7.4, 7.7

Copyright (C) University of Cambridge

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 5 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

Written by: Philip Hazel <ph10@cam.ac.uk>

University of Cambridge Computing Service,

Cambridge, England. Phone: +44 1223 334714.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the University of Cambridge nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

PROTOCOL BUFFER

Copyright (C) 2008, Google Inc

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Code generated by the Protocol Buffer compiler is owned by the owner of the input file used when generating it. This code is not standalone and requires a support library to be linked with it. This support library is itself covered by the above license.

QT 4.6.1

Copyright (C) 2009, Nokia Corporation and/or its subsidiary(-ies)

GNU LESSER GENERAL PUBLIC LICENSE v.2,1

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6,)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA. Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990

Ty Coon, President of Vice

That's all there is to it!

RFC1321-BASED (RSA-FREE) MD5 LIBRARY

Copyright (C) 1999, 2002, Aladdin Enterprises

TINICONV 1.0.0

Copyright (C) Free Software Foundation, Inc

----

http://sourceforge.net/projects/tiniconv/

GNU LESSER GENERAL PUBLIC LICENSE v.2,1

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6,)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA. Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990

Ty Coon, President of Vice

That's all there is to it!

WINDOWS TEMPLATE LIBRARY 7.5

Copyright (C) 2005, Microsoft Corporation

Common Public License Version 1,0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

WINDOWS TEMPLATE LIBRARY 8.0

Copyright (C) Microsoft Corporation

ZLIB 1.2, 1.2.2

Copyright (C) Jean-loup Gailly and Mark Adler

SONSTIGE INFORMATIONEN

Zusatzinformationen zum Code von Drittherstellern

Für die Überprüfung elektronischer digitaler Signaturen wird die Krypto-Bibliothek (Programmbibliothek zum Informationsschutz - PBSI) "Agava-S" verwendet, die von OOO "R-Alpha" entwickelt wurde.

Dieses Produkt enthält Programme oder kann Programme enthalten, die nach der freien GNU-Lizenz oder anderen vergleichbaren Open Source-Lizenzen an den Benutzer lizenziert (oder sublizenziert) werden, die dem Benutzer neben sonstigen Rechten gestatten, bestimmte Programme oder deren Teile zu kopieren, zu modifizieren und zu verteilen sowie auf den Quellcode zuzugreifen ("Open Source Software"). Falls es solche Lizenzen erforderlich machen, dass für jedwede Software, die an jemanden in ausführbarem Binärformat geliefert wird, diesen Nutzern der Quellcode ebenfalls verfügbar gemacht wird, dann soll der Quellcode zur Verfügung gestellt werden, indem ein diesbezügliches Ersuchen an source@kaspersky.com gesendet wird, oder der Quellcode wird mit der Software geliefert.

SACHREGISTER

A

Anti-Banner
- Liste mit erlaubten Banneradressen ... 137
- Weiße Liste ... 137

Anti-Spam
- Erweiterung für Microsoft Office Outlook ... 134
- Erweiterung für Microsoft Outlook Express ... 134
- Erweiterung für The Bat! ... 135
- Filterung von E-Mails auf dem Server ... 132
- Liste mit erlaubten Absendern ... 128
- Liste mit erlaubten Phrasen ... 126
- Thunderbird-Erweiterung ... 135

B

Backup
- Backup-Aufgabe erstellen ... 173
- Backup-Aufgabe starten ... 174
- Daten einer Sicherungskopie anzeigen ... 176
- Daten wiederherstellen ... 174
- Ereignisbericht anzeigen ... 177
- Sicherungskopien suchen ... 175
- Speicher anlegen ... 171
- Speicher leeren ... 172
- Speicher löschen ... 173
- Speicher verbinden ... 172

Berichte ... 239

D

Datenverschlüsselung
- Container anlegen ... 187
- Container verbinden und trennen ... 188
- Dateien zu einem Container hinzufügen ... 189
- Einstellungen eines Containers anpassen ... 189

F

Firewall
- Adressenbereich eines Netzwerks erweitern ... 152
- Assistent für neue Regeln ... 153

K

Kategorien der erkennbaren Bedrohungen ... 227

Kindersicherung
- Beschränkung für die Verwendung des Computers ... 181
- Besuch von Webseiten ... 182
- Download von Dateien aus dem Internet ... 182
- Korrespondenz über Instant Messenger ... 183
- Modus für sichere Suche ... 182
- Parameter aktivieren und anpassen ... 179
- Parameter exportieren/importieren ... 179
- Persönliche Informationen senden ... 185
- Schlüsselwörter suchen ... 186
- Start von Programmen und Spielen ... 181
- Zeitliche Beschränkung für die Verwendung des Internets ... 181

L

Lizenz

Lizenzvertrag 42

M

Mail-Manager
Anti-Spam 132

P

Password Manager
Benutzerkonto 198
Benutzername 203
Gruppe von Benutzerkonten 203
Kennwörter importieren/exportieren 206
Kennwörter suchen 205
Kennwort-Generator 223
Master-Kennwort ändern 219
Methode zur Datenverschlüsselung 217
Persönliche Daten 205
Portable Version 224
Schnellstart von Programmfunktionen 214
Titelleisten-Schaltfläche 221
Visitenkarte 204
Zugriff auf die Kennwort-Datenbank 196

Programmkontrolle
Rechte erben 144
Regeln für die Programmkontrolle 142

Programm-Update 93

R

Rechte erben
Programmkontrolle 144

Regeln für die Programmkontrolle
Programmkontrolle 142

S

Schutz vor Netzwerkangriffen
Arten der erkennbaren Netzwerkangriffe 155

Schutzmodus auswählen
Sichere Umgebung 166

Sichere Umgebung
Schutzmodus auswählen 166
Verknüpfung erstellen 166

U

Update
Aus einem lokalen Ordner 96
Nach Zeitplan 97
Proxyserver 98
Regionsoptionen 96
Rollback zum vorherigen Update 98
Updatequelle 95

V

Verknüpfung erstellen
Sichere Umgebung 166

Verwaltung
Backup 194
Fernverwaltung anpassen 191
Kindersicherung verwalten 193
Lizenzen verwalten 194
Netzwerksicherheit analysieren 69
Schutzkomponenten verwalten 193

Untersuchung auf Viren und Schwachstellen 192
Update 192

Z

Zusätzliche Funktionen
Assistent zum Löschen von Aktivitätsspuren 235
Browser-Konfiguration 238
Nicht verwendete Informationen löschen 236
Unwiderrufliches Löschen von Daten 234